(51) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年6 月24 日 (24.06.2004)

PCT

(10) 国際公開番号
WO 2004/053699 A2

(51) 国際特許分類[7]: G06F 12/14, H04L 9/08, G11B 20/10

(21) 国際出願番号: PCT/JP2003/015525

(22) 国際出願日: 2003 年12 月4 日 (04.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-355114 2002 年12 月6 日 (06.12.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 木谷 聡 (KITANI,Satoshi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 杉浦 正知, 外(SUGIURA,Masatomo et al.); 〒171-0022 東京都 豊島区 南池袋 2丁目49番 7号 池袋パークビル７階 Tokyo (JP).

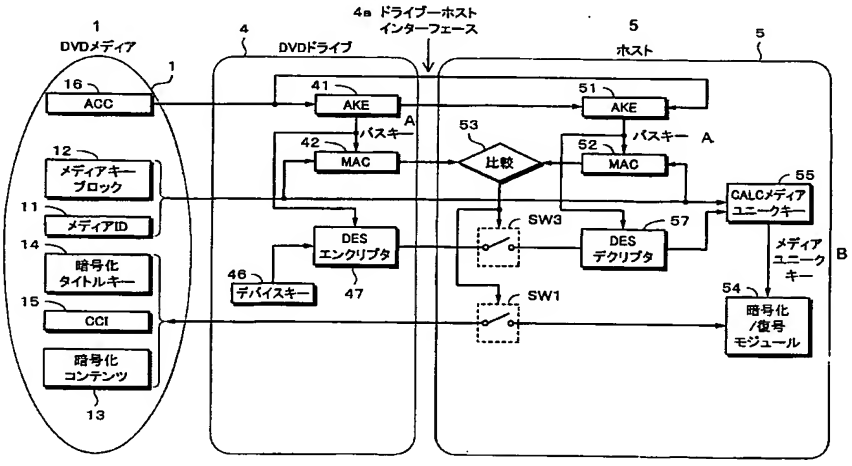
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

[続葉有]

(54) Title: RECORDING/REPRODUCTION DEVICE, DATA PROCESSING DEVICE, AND RECORDING/REPRODUCTION SYSTEM

(54) 発明の名称: 記録再生装置、データ処理装置および記録再生処理システム



1...DVD MEDIUM
12...MEDIUM KEY BLOCK
11...MEDIUM ID
14...ENCRYPTION TITLE KEY
13...ENCRYPTION CONTENT
4a...DRIVE-HOST INTERFACE
4...DVD DRIVE
A...BUS KEY

46...DEVICE KEY
47...DES ENCRYPTER
5...HOST
53...COMPARISON
55...CALC MEDIUM UNIQUE KEY
57...DES DECRYPTER
B...MEDIUM UNIQUE KEY
54...ENCRYPTION/DECRYPTION MODULE

(57) Abstract: A device key (46) is mounted on a drive (4) side. In order to securely send the device key (46) to a host (5), the device key (46) is encrypted by a bus key. At the host (5) side, the device key is decrypted by the bus key. A medium unique key calculation block (55) calculates the medium unique key from an MKB (12), a medium ID, and a decrypted device key (46). In the calculation block (55), when the calculated medium key becomes

[続葉有]

WO 2004/053699 A2

TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書なし；報告書を受け取り次第公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

a predetermined value, the drive (4) is revoked and the processing is terminated. The medium unique key is supplied to an encryption/decryption module (54) and a content key is obtained from an encryption title key (14) and a CCI (15). By using the content key, the encrypted content is decrypted and the content to be recorded is encrypted.

(57) 要約: デバイスキー４６がドライブ４側に実装される。デバイスキー４６をセキュアにホスト５に伝送するために、デバイスキー４６がバスキーで暗号化される。ホスト５側で、バスキーでデバイスキーが復号される。メディアユニークキー演算ブロック５５がＭＫＢ１２とメディアＩＤと復号されたデバイスキー４６とからメディアユニークキーを演算する。演算ブロック５５において、計算されたメディアキーが所定の値となる場合には、ドライブ４がリボークされ、処理が停止される。メディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められ、コンテンツキーを使用して暗号化コンテンツが復号され、記録されるコンテンツが暗号化される。

明　細　書

記録再生装置、データ処理装置および記録再生処理システム

技術分野

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される記録再生装置、データ処理装置および記録再生処理システムに関する。

背景技術

近年開発されたＤＶＤ(Digital Versatile Disc)等の記録媒体では、１枚の媒体に例えば映画１本分の大量のデータをディジタル情報として記録することが可能である。このように映像情報等をディジタル情報として記録することが可能となってくると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

ＤＶＤ－Video では、コピープロテクション技術としてＣＳＳ(Content Scrambling System) が採用されている。ＣＳＳは、ＤＶＤメディアに対する適用のみが認可されており、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ＋Ｒ、ＤＶＤ＋ＲＷ等の記録型ＤＶＤでのＣＳＳの利用がＣＳＳ契約によって禁止されている。したがって、ＤＶＤ－Video の内容を記録型ＤＶＤへのまるごとコピー（ビットバイビットコピー）は、ＣＳＳ契約上では、認められた行為ではない。

しかしながら、ＣＳＳの暗号方式が破られる事態が発生した。ＣＳＳの暗号化を解除してＤＶＤ－Video の内容を簡単にハードディスクにコピーする「ＤｅＣＳＳ」と呼ばれる違法なソフトウェアがインターネット上で配布された。「ＤｅＣＳＳ」が出現した背景には、本来

耐タンパー化が義務付けられているはずのＣＳＳ復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にＣＳＳアルゴリズム全体が解読された経緯がある。

ＣＳＳの後に、ＤＶＤ－Audio 等のＤＶＤ－ＲＯＭの著作権保護技術であるＣＰＰＭ(Content Protection for Pre-Recorded Media)、並びに記録型ＤＶＤ、メモリカードに関する著作権保護技術ＣＲＰＭ(Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、データをまるごとコピーしても再生を制限できる特徴を有している。ＤＶＤに関する著作権保護の方法に関しては、下記の非特許文献１に説明され、ＣＲＰＭは、ライセンス管理者である米4C Entity,LLC が配布する下記の資料に説明されている。

山田，「ＤＶＤを起点に著作権保護空間を広げる」，日経エレクトロニクス 2001.8.13,p.143-153

"Content Protection for Recordable Media Specification DVD Book"、インターネット＜ＵＲＬ：http://www.4Centity.com/＞

パーソナルコンピュータ（以下、適宜ＰＣと略す）環境下では、ＰＣとドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。アプリケーションソフトウェアがリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

著作権保護技術をＰＣ上で実行されるアプリケーションプログラム

へ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がない。その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。ＣＳＳの場合は、結果として破られてしまった。ＣＳＳの後に提案されたＣＰＰＭおよび記録型ＤＶＤに関する著作権保護技術ＣＲＰＭにおいても、ＰＣでのソフトウェア実装に関する問題解決に至る技術的方法の提案がなされていない。

この発明の目的は、ＰＣ環境下でも著作権保護技術の安全性を確保することである。すなわち、正規のライセンスを受けないドライブの作成を防止し、さらに、確実にリボケーションを行うことが可能な記録再生装置、データ処理装置および記録再生処理システムを提供することにある。

発明の開示

上述した課題を解決するために、この発明の第１の態様は、記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータを記録する記録部および記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第２の情報が格納される格納部と、

記録媒体固有の第１の情報と格納部に格納された第２の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

を有する記録再生装置である。

この発明の第2の態様は、少なくとも格納部に格納された第2の情報と記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有するデータ処理装置に対して、接続部が格納部に格納された第2の情報を送る記録再生装置である。

この発明の第3の態様は、格納部に格納された第2の情報と記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置である。

この発明の第4の態様は、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータを記録する記録部および記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーシソトウェア固有にのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報が格納される格納部と、

記録媒体固有の第1の情報と格納部に格納された第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

少なくとも接続部を介してデータ処理装置から送られ、格納部に格納された第2の情報と、記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当なアプリケーションソフトウェア固有の

情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置である。

この発明の第5の態様は、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報を有するとともに、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

接続部を介して記録再生装置から送られた、記録媒体固有の第1の情報と電子機器またはアプリケーションソフトウェア固有の第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部と

を有するデータ処理装置である。

この発明の第6の態様は、接続部を介して記録再生装置から送られた第2の情報と、記録媒体固有の第1の情報とを用いて、第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有するデータ処理装置である。

この発明の第7の態様は、少なくとも記録再生装置に格納された第2の情報と、記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置と接続するデータ処理装置である。

この発明の第8の態様は、正当なアプリケーションソフトウェアにのみ与えられるアプリケーションソフトウェア固有の第2の情報を有する格納部と、

記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

記録媒体固有の第１の情報と格納部に格納された第２の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部とを有し、

格納部に格納された第２の情報が正当なアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置に対して、格納部に格納された第２の情報を送るデータ処理装置である。

この発明の第９の態様は、記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方が可能であると共に、正当な電子機器またはアプリケーシソトウェア固有にのみ与えられる電子機器またはアプリケーションソフトウェア固有の第２の情報を有する記録再生装置と、

少なくとも格納された第２の情報と、記録媒体固有の第１の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と

を有する記録再生処理システムである。

この発明の第１０の態様は、データ処理装置が記録媒体固有の第１の情報と格納された第２の情報を用いて、当該格納された第２の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生処理システムである。

この発明の第１１の態様は、記録再生装置が記録媒体固有の第１の情報と格納された第２の情報を用いて、当該格納された第２の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生処理システムである。

この発明の第１２の態様は、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報として格納された第２の情報を有するとともに、記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と、

格納された第２の情報と、記録媒体固有の第１の情報とに基づいて生成された鍵を用いてデータの暗号化、または暗号化されたデータの復号が可能なデータ処理装置とからなり、

格納された第２の情報が正当なアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置に対して、データ処理装置が格納部に格納された第２の情報を送る記録再生処理システムである。

この発明の第１３の態様は、不正な電子機器を無効化するための第１の情報と、コンテンツ毎に異なる第２の情報と、暗号化単位毎に定義可能な第３の情報と、スタンパ毎に異なる識別データとが記録された記録媒体へ暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第４の

情報が格納される格納部と、

上記第1の情報と上記第4の情報とから当該格納された第4の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であるかを判定するリボーク処理部と、

上記リボーク処理部で上記第4の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であると判定された場合に、上記第1の情報、上記第4の情報、上記第2の情報および上記識別データから、個々の記録媒体毎に固有の中間鍵情報を求める演算部と有する記録再生装置である。

この発明では、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第2の情報例えばデバイスキーが記録再生装置に格納されている。したがって、デバイスキーを外部から読み取ることが不可能となり、データ処理装置にインストールされるアプリケーションは、著作権保護技術に関するデータを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。また、記録媒体を扱う正当な記録再生装置となるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン装置の作成を防止できる効果がある。

この発明では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算が記録再生装置内に実装されている。その結果、データ処理装置にインストールされるアプリケーションは、著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に

対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

図面の簡単な説明

第１図は、先に提案されているレコーダ、プレーヤおよびＤＶＤメディアからなるシステムを説明するためのブロック図である。

第２図は、ＰＣベースのＤＶＤメディア記録再生システムを説明するためのブロック図である。

第３図は、第２図のシステムにおけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

第４図は、第２図のシステムにおける認証動作を説明するためのフローチャートである。

第５図は、この発明の第１の実施形態によるＰＣベースのＤＶＤメディア記録再生システムのブロック図である。

第６図は、この発明の第１の実施形態におけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

第７図は、この発明の第２の実施形態によるＰＣベースのＤＶＤメディア記録再生システムのブロック図である。

第８図は、この発明の第３の実施形態によるＰＣベースのＤＶＤメディア記録再生システムのブロック図である。

第９図は、この発明の第３の実施形態におけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

第１０図は、この発明の第４の実施形態によるＰＣベースのＤＶＤメディア記録再生システムのブロック図である。

第１１図は、この発明の第４の実施形態におけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

第１２図は、この発明の第５の実施形態によるＰＣベースのＤＶＤメディア記録再生システムのブロック図である。

第１３図は、この発明の第６の実施形態によるＰＣベースのＤＶＤメディア記録再生システムのブロック図である。

第１４図は、この発明の第６の実施形態におけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

第１５図は、この発明の第７の実施形態によるＰＣベースのＤＶＤメディア記録再生システムのブロック図である。

第１６図は、この発明の第７の実施形態におけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

第１７図は、この発明の第８の実施形態によるＰＣベースの書き込み可能なメディアの記録再生システムのブロック図である。

第１８図は、この発明の第９の実施形態によるＰＣベースのＲＯＭタイプのメディアの再生システムのブロック図である。

発明を実施するための最良の形態

この発明の理解の容易のために、最初に第１図を参照して著作権保護技術例えばＤＶＤ用ＣＰＲＭのアーキテクチャについて説明する。第１図において、参照符号１が例えばＣＰＲＭ規格に準拠したＤＶＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＡＭ等の記録型ＤＶＤメディアを示す。参照符号２が例えばＣＰＲＭ規格に準拠したレコーダを示す。参照符号３が例えばＣＰＲＭ規格に準拠したプレーヤを示す。レコーダ２およびプレーヤ３は、機器またはアプリケーションソフトウェアである。

未記録ディスクの状態において、ＤＶＤメディア１の最内周側のリードインエリアのＢＣＡ(Burst Cutting Area)またはＮＢＣＡ(Narrow Burst Cutting Area) と称されるエリアには、メディアＩＤ１１が

記録されている。リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、ＭＫＢと適宜略す）１２が予め記録されている。メディアＩＤ１１は、個々のメディア単位例えばディスク１枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディアＩＤ１１は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロックＭＫＢは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアＩＤおよびメディアキーブロックは、記録媒体固有の第１の情報である。

ディスク１の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ１３が記録される。暗号化方式としては、Ｃ２(Cryptomeria Ciphering) が使用される。

ＤＶＤメディア１には、暗号化タイトルキー１４およびＣＣＩ(Copy Control Information)１５が記録される。暗号化タイトルキー１４は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。ＣＣＩは、コピーノーモア、コピーワンス、コピーフリー等のコピー制御情報である。

レコーダ２は、デバイスキー２１、プロセスＭＫＢ２２、Ｃ２＿Ｇ２３、乱数発生器２４、Ｃ２＿Ｅ２５、Ｃ２＿Ｇ２６およびＣ２＿ＥＣＢＣ２７の構成要素を有する。プレーヤ３は、デバイスキー３１、プロセスＭＫＢ３２、Ｃ２＿Ｇ３３、Ｃ２＿Ｄ３５、Ｃ２＿Ｇ３６およびＣ２＿ＤＣＢＣ３７の構成要素を有する。

デバイスキー２１、３１は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケ

ーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。ＤＶＤメディア１から再生されたＭＫＢ１２とデバイスキー２１とがプロセスＭＫＢ２２において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ２におけるのと同様に、プレーヤ３においても、ＭＫＢ１２とデバイスキー３１とがプロセスＭＫＢ３２において演算され、リボケーションされたかどうかの判別がなされる。

プロセスＭＫＢ２２、３２のそれぞれにおいて、ＭＫＢ１２とデバイスキー２１、３１からメディアキーが算出される。ＭＫＢ１２の中にレコーダ２またはプレーヤ３のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ２またはプレーヤ３が正当なものでないと判断される。すなわち、そのようなレコーダ２またはプレーヤ３がリボケーションされる。

Ｃ２＿Ｇ２３、３３は、それぞれ、メディアキーとメディアＩＤとを演算し、メディアユニークキーを導出する処理である。

乱数発生器（ＲＮＧ：Random Number Generator）２４は、タイトルキーの生成に利用される。乱数発生器２４からのタイトルキーがＣ２＿Ｅ２５に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー１４がＤＶＤメディア１に記録される。

プレーヤ３では、ＤＶＤメディア１から再生された暗号化タイトルキー１４とメディアユニークキーとがＣ２＿Ｄ３５に供給され、暗号化タイトルキーがメディアユニークキーで復号化され、タイトルキーが得られる。

レコーダ２においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ２６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿Ｅ

ＣＢＣ２７に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１３がＤＶＤメディア１に記録される。

プレーヤ３においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ３６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＤＣＢＣ３７に供給され、ＤＶＤメディア１から再生された暗号化コンテンツ１３がコンテンツキーを鍵として復号される。

第１図の構成において、レコーダ２による記録の手順について説明する。レコーダ２は、ＤＶＤメディア１からＭＫＢ１２を読み出し、プロセスＭＫＢ２２によってデバイスキー２１とＭＫＢ１２とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー２１（レコーダ２の機器またはアプリケーション）がＭＫＢによってリボークされたと判定される。レコーダ２は、以後の処理を中断し、ＤＶＤメディア１への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

レコーダ２は、ＤＶＤメディア１からメディアＩＤ１１を読み、メディアキーと共にメディアＩＤをＣ２＿Ｇ２３に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器２４で発生させたタイトルキーがＣ２＿Ｅ２５で暗号化され、暗号化タイトルキー１４としてＤＶＤメディア１に記録される。タイトルキーとコンテンツのＣＣＩ情報がＣ２＿Ｇ２６で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをＣ２＿ＥＣＢＣ２７で暗号化し、ＤＶＤメディア１上に暗号化コンテンツ１３としてＣＣＩ１５と共に記録する。

プレーヤ３による再生の手順について説明する。最初にＭＫＢ１２をＤＶＤメディア１から読み出す。デバイスキー３１とＭＫＢ１２を演算し、リボケーションの確認がなされる。デバイスキー３１、すな

わち、プレーヤ３の機器またはアプリケーションがリボークされない場合には、メディアＩＤを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー１４とメディアユニークキーからタイトルキーが演算される。タイトルキーとＣＣＩ１５とがＣ２＿Ｇ３６に入力され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＤＣＢＣ３７に入力され、コンテンツキーを鍵として、ＤＶＤメディア１から再生された暗号化コンテンツ１３に対してＣ２＿ＤＣＢＣ３７の演算が施される。その結果、暗号化コンテンツ１３が復号される。

このように、コンテンツの復号に必要なコンテンツキーを得るためには、ＤＶＤメディアの１枚毎に異なるメディアＩＤが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアＩＤがオリジナルのメディアＩＤと異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

上述した第１図の構成は、記録再生機器として構成されたものである。この発明は、ＤＶＤメディア１に対するコンテンツ保護処理をＰＣ環境下で扱う場合に適用される。第２図を参照して現行の方式によるＰＣとドライブの役割分担を示す。第２図において、参照符号４が上述したＣＰＲＭ規格に準拠したＤＶＤメディア１を記録および再生する記録再生装置としてのＤＶＤドライブを示す。

参照符号５がデータ処理装置としてのホスト例えばＰＣを示す。ホスト５は、ＤＶＤメディア１に記録可能で、ＤＶＤメディア１から再生可能なコンテンツを扱うことができ、且つＤＶＤドライブ４と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばＰＣに対してアプリケーションソフトウェアがインス

トールされることによってホスト５が構成される。

ＤＶＤドライブ４とホスト５との間がインターフェース４ａで接続されている。インターフェース４ａは、ＡＴＡＰＩ(AT Attachment with Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers) １３９４等である。

ＤＶＤメディア１には、メディアＩＤ１１、メディアキーブロック１２およびＡＣＣ(Authentication Control Code) が予め記録されている。ＡＣＣは、ＤＶＤドライブ４とホスト５との間の認証がＤＶＤメディア１によって異なるようにするために予めＤＶＤメディア１に記録されたデータである。

ＤＶＤドライブ４は、ＡＣＣ１６をＤＶＤメディア１から読み出す。ＤＶＤメディア１から読み出されたＡＣＣ１６がＤＶＤドライブ４のＡＫＥ(Authentication and Key Exchange) ４１に入力されると共に、ホスト５へ転送される。ホスト５は、受け取ったＡＣＣをＡＫＥ５１に入力する。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣの値とから認証動作の度に異なる値となる共通のセッションキー（バスキーと称する）を生成する。

バスキーがＭＡＣ(Message Authentication Code) 演算ブロック４２および５２にそれぞれ供給される。ＭＡＣ演算ブロック４２および５２は、ＡＫＥ４１および５１でそれぞれ得られたバスキーをパラメータとして、メディアＩＤおよびメディアキーブロック１２のＭＡＣを計算するプロセスである。ＭＫＢとメディアＩＤの完全性(integrity) をホスト５が確認するために利用される。

ＭＡＣ４２および５２によってそれぞれ計算されたＭＡＣがホスト５の比較５３において比較され、両者の値が一致するかどうかが判定

される。これらのＭＡＣの値が一致すれば、ＭＫＢとメディアＩＤの完全性が確認されたことになる。比較出力でスイッチＳＷ１が制御される。

スイッチＳＷ１は、ＤＶＤドライブ４のＤＶＤメディア１の記録または再生経路と、ホスト５の暗号化／（または）復号モジュール５４との間の信号路をＯＮ／ＯＦＦするものとして示されている。スイッチＳＷ１は、信号路のＯＮ／ＯＦＦを行うものとして示されているが、より実際には、ＯＮの場合にホスト５の処理が継続し、ＯＦＦの場合にホスト５の処理が停止することを表している。暗号化／復号モジュール５４は、メディアユニークキーと暗号化タイトルキーとＣＣＩとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ１３へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ１３を復号する演算ブロックである。

メディアユニークキー演算ブロック５５は、ＭＫＢ１２とメディアＩＤとデバイスキー５６とからメディアユニークキーを演算する演算ブロックである。第１図に示すレコーダまたはプレーヤと同様に、デバイスキーとＭＫＢ１２とからメディアキーが演算される。メディアキーとメディアＩＤ１１とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック５５は、リボケーションを行うリボーク処理部としての機能も有する。

記録時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされる。暗号化／復号モジュール５４からスイッチＳＷ１を通じてドライブ４に対して、暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５が供給され、ＤＶＤメディア１に対

してそれぞれ記録される。再生時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされる。ＤＶＤメディア１からそれぞれ再生された暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５がスイッチＳＷ１を通じてホスト５の暗号化／復号モジュール５４に対して供給され、暗号化コンテンツが復号される。

第３図は、第２図に示す現行のＰＣ環境下のＤＶＤメディアを利用するシステムにおいて、ＤＶＤメディア１と、ＤＶＤドライブ４と、ホスト５との間の信号の授受の手順を示す。ホスト５がＤＶＤドライブ４に対してコマンドを送り、ＤＶＤドライブ４がコマンドに応答した動作を行う。

ホスト５からの要求に応じてＤＶＤメディア１上のＡＣＣがシークされ、読み出される（ステップＳ１）。次のステップＳ２において、読み出されたＡＣＣがＡＫＥ４１に入力されると共に、ホスト５へ転送され、ホスト５では、受け取ったＡＣＣがＡＫＥ５１へ入力される。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣ１６の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをＤＶＤドライブ４とホスト５が共有する。相互認証が成立しなかった場合では、処理が中断する。

認証動作は、電源のＯＮまたはＯＦＦ時並びにディスクの交換時には、必ず行われる。記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

認証が成功すると、ステップＳ３において、ホスト５がＤＶＤドライブ４に対して、ＤＶＤメディア１からのＭＫＢ（メディアキーブロ

ック）パック＃０の読み出しを要求する。ＭＫＢは、パック０～パック１５の１６セクタが１２回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

ＤＶＤドライブ４がステップＳ４においてＭＫＢのパック＃０を読みに行き、ステップＳ５において、パック＃０が読み出される。ＤＶＤドライブ４は、モディフアイドＭＫＢをホスト５へ戻す（ステップＳ６）。ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加してホスト５へデータを転送する。パック＃０以外の残りのＭＫＢパックの要求と、ＤＶＤドライブ４の読み出し動作と、モディフアイドＭＫＢパックの転送動作とがＭＫＢのパックがなくなるまで、例えばパック＃１５が読み出され、ホスト５へ転送されるまで、ステップＳ７およびＳ８によって繰り返しなされる。

ホスト５がＤＶＤドライブ４に対してメディアＩＤを要求する。ＤＶＤドライブ４がＤＶＤメディア１に記録されているメディアＩＤを読みに行き、ステップＳ１１において、メディアＩＤが読み出される。ＤＶＤドライブ４は、メディアＩＤを読み出す際に、バスキーをパラメータとしてそのＭＡＣ値を計算する。ＤＶＤドライブ４は、ステップＳ１２において、読み出されたメディアＩＤに対してＭＡＣ値ｍ１を付加してホスト５へデータを転送する。

ホスト５では、ＤＶＤドライブ４から受け取ったＭＫＢ１２およびメディアＩＤ１１からバスキーをパラメータとして再度ＭＡＣ値を計算し、計算したＭＡＣ値とＤＶＤドライブ４から受け取ったＭＡＣ値とを比較５３で比較する。両者が一致したならば、正しいＭＫＢおよびメディアＩＤを受け取ったと判定して、スイッチＳＷ１をＯＮに設定して処理を先に進める。逆に両者が一致しなかったならば、ＭＫＢ

およびメディアＩＤが改ざんされたものと判定して、スイッチＳＷ１をＯＦＦに設定して処理を中断する。

ステップＳ１３において、ホスト５がＤＶＤドライブ４に対して暗号化コンテンツを要求し、ステップＳ１４において、ＤＶＤドライブ４が暗号化コンテンツを読み出し、ステップＳ１３において、読み出した暗号化コンテンツがホスト５に転送される。ホスト５のメディアユニークキー演算ブロック５５では、デバイスキー５６とＭＫＢ１２とメディアＩＤ１１とによってメディアユニークキーが計算される。メディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められる。コンテンツキーを鍵としてＤＶＤメディア１から読み出された暗号化コンテンツが復号される。ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

第４図のフローチャートにおいて、ステップＳＴ１は、ＭＡＣ演算ブロック４２でバスキーをパラメータとして求められたＭＡＣ計算値と、ＭＡＣ演算ブロック５３でバスキーをパラメータとして求められたＭＡＣ計算値とを比較するステップである。両者が一致すれば、スイッチＳＷ１がステップＳＴ２においてＯＮとされる。両者が一致しない場合では、スイッチＳＷ１がステップＳＴ３においてＯＦＦとされ、処理が停止する。

第２図に示すようなＰＣ環境下のシステムに対して適用されるこの発明の第１の実施形態を第５図に示す。第１の実施形態は、ホスト５の側で秘密情報とされているデバイスキーをＤＶＤドライブ４側に記憶するようにしたものである。デバイスキーは、上述したように、リボケーション動作とメディアキーの導出に使用される情報である。

第５図において、参照符号４６がＤＶＤドライブ４側に記憶された

デバイスキーである。デバイスキー４６をセキュアにホスト５に伝送するために、デバイスキー４６が暗号化例えばＤＥＳ(Data Encryption Standard)エンクリプタ４７に入力され、バスキーで暗号化される。暗号化デバイスキーがドライブホストインターフェース４ａを通じてホスト５へ転送される。

比較５３においてＭＡＣ値が一致すると検出された場合、すなわち、完全性が確認できた場合にのみＯＮするスイッチＳＷ２を介して暗号化デバイスキーがＤＥＳデクリプタ５７に入力される。スイッチＳＷ２は、信号路のＯＮ／ＯＦＦを行うものとして示されているが、より実際には、スイッチＳＷ１と同様に、ＯＮの場合にホスト５の処理が継続し、ＯＦＦの場合にホスト５の処理が停止することを表している。ＤＥＳデクリプタ５７には、バスキーが供給され、デバイスキーが復号される。

復号されたデバイスキーがメディアユニークキー演算ブロック５５に供給され、ＭＫＢ１２とメディアＩＤとデバイスキー４６とからメディアユニークキーが演算される。ＭＫＢ１２とデバイスキー４６とを使用してメディアキーが計算され、メディアＩＤとメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキー演算ブロック５５において、計算されたメディアキーが所定の値となる場合には、デバイスキー、すなわち、ＤＶＤドライブ４がリボークされ、処理が停止される。メディアユニークキー演算ブロック５５は、リボーク処理部の機能を有している。

メディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められる。コンテンツキーを使用してＤＶＤメディア１から読み出された暗号化コンテンツが復号され、ＤＶＤメディア１に対して記録されるコ

ンテンツが暗号化される。

第６図は、第１の実施形態の処理の手順を示す。ＡＣＣのシークおよびリード（ステップＳ２１）からメディアＩＤとｍ１をリターン（ステップＳ３２）までの処理は、第３図に示すものと同様であるので、この処理については、簡単に説明する。ステップＳ２１では、ＡＣＣがシークされ、読み出され、ステップＳ２２において認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。

ステップＳ２３において、ホスト５がＭＫＢ（メディアキーブロック）パック＃０の読み出しをＤＶＤドライブ４に要求し、ＤＶＤドライブ４がステップＳ２４においてＭＫＢパック＃０を読みに行き、ステップＳ２５において、パック＃０が読み出される。ステップＳ２６で、ＤＶＤドライブ４は、ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加したデータ（モディファイドＭＫＢ）をホスト５へ戻す。ステップＳ２７およびＳ２８において、パック＃０以外の残りのＭＫＢパックの要求と、読み出し動作と、転送動作とがなされる。

ホスト５がメディアＩＤを要求し（ステップＳ２９）、ＤＶＤドライブ４がメディアＩＤを読みに行き（ステップＳ３０）、ステップＳ３１において、メディアＩＤが読み出される。ＤＶＤドライブ４は、メディアＩＤを読み出す際に、バスキーをパラメータとしてそのＭＡＣ値を計算し、ステップＳ３２において、読み出されたメディアＩＤに対してＭＡＣ値ｍ１を付加してホスト５へデータを転送する。

ホスト５では、ＤＶＤドライブ４から受け取ったＭＫＢ１２およびメディアＩＤ１１からバスキーをパラメータとして再度ＭＡＣ値を計算する。計算したＭＡＣ値とＤＶＤドライブ４から受け取ったＭＡＣ

値とが一致したならば、正しいＭＫＢおよびメディアＩＤを受け取ったと判定して、スイッチＳＷ１をＯＮに設定して処理を先に進める。逆に両者が一致しなかったならば、ＭＫＢおよびメディアＩＤが改ざんされたものと判定して、スイッチＳＷ１をＯＦＦに設定して処理を停止する。

ステップＳ３３において、ホスト５がＤＶＤドライブ４に対してデバイスキーを要求する。ＤＶＤドライブ４は、デバイスキー４６をＤＥＳエンクリプタ４７によって暗号化し、暗号化デバイスキーをホスト５に送る（ステップＳ３４）。ホスト５は、バスキーを使用してＤＥＳデクリプタ５７によってデバイスキーを復号する。

ステップＳ３５において、ホスト５がＤＶＤドライブ４に対して暗号化コンテンツを要求し、ステップＳ３６において、ＤＶＤドライブ４が暗号化コンテンツを読み出し、ステップＳ３５において、読み出した暗号化コンテンツがホスト５に転送される。ホスト５のメディアユニークキー演算ブロック５５では、デバイスキー４６とＭＫＢ１２とメディアＩＤ１１とによってメディアユニークキーが計算される。メディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化コンテンツが復号され、また、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

上述した第１の実施形態では、著作権保護技術に関する秘密情報であるデバイスキーがＤＶＤドライブ４内に実装されている。例えばフラッシュメモリ等のＬＳＩ(Large Scale Integrated Circuit ：大規模集積回路）内にデバイスキーが実装される。ＬＳＩ内のデバイスキーを外部から読み取ることが不可能とされている。ホスト５にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報を持つ必要がなくなる。それによって、ソフトウェアの

リバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

ＤＶＤメディア１を扱う正当なドライブとなるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

ＰＣ環境下で実施されるこの発明の第２の実施形態を第７図に示す。第２の実施形態は、ホスト５の側で秘密情報とされているデバイスキーを二つの要素に分解し、その内の一方の要素をＤＶＤドライブ４側に記憶するようにしたものである。

第７図において、参照符号４６ａがＤＶＤドライブ４側に記憶されたデバイスキーの前半部である。デバイスキーの前半部とは、デバイスキーの後半部と組み合わされることによって完全なデバイスキーを構成するデバイスキーの一部分のことである。デバイスキーの前半部４６ａが暗号化例えばＤＥＳエンクリプタ４７に入力され、バスキーで暗号化される。暗号化デバイスキーの前半部がドライブホストインターフェース４ａを通じてホスト５へ転送される。

比較５３においてＭＡＣ値が一致すると検出された場合にのみＯＮするスイッチＳＷ２を介して暗号化デバイスキーの前半部がＤＥＳデクリプタ５７に入力される。ＤＥＳデクリプタ５７には、バスキーが供給され、デバイスキーの前半部がＤＥＳデクリプタ５７によって復号される。

参照符号５６ａがデバイスキーの後半部を示す。ＤＥＳデクリプタ５７によって復号されたデバイスキーの前半部４６ａとデバイスキーの後半部５６ａとがデバイスキー合成部５８に入力され、両者が合成されることで、デバイスキーが得られる。

得られたデバイスキーがメディアユニークキー演算ブロック５５に供給され、ＭＫＢ１２とメディアＩＤとデバイスキー４６とからメディアユニークキーが演算される。そして、メディアユニークキーが暗号化／復号モジュール５４に供給される。暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められ、コンテンツキーを使用してＤＶＤメディア１から読み出された暗号化コンテンツが復号され、また、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

上述した第２の実施形態は、デバイスキーを二つの要素に分解している点を除くと、第１の実施形態と同様のものであり、処理の手順は、第６図と同様のものであり、その図示については省略する。

第２の実施形態では、著作権保護技術に関するデータとしてデバイスキーの一部がドライブ４内に実装されている。例えばＬＳＩ内にデバイスキーの一部が実装される。その結果、ホスト５にインストールされるアプリケーションは、著作権保護技術に関するデータを一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

ＤＶＤメディア１を扱う正当なドライブとなるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。デバイスキーの前半部４６ａとその後半部５６ａが共に正しい場合にのみ、電子機器またはアプリケーションソフトウェアが正当なものとされるので、ＤＶＤドライブ４およびホスト５の両方について、リボーク処理を行うことが可能となる。

第８図は、この発明の第３の実施形態を示す。第３の実施形態では、デバイスキー４６をＤＶＤドライブ４が持ち、参照符号４８で示すメディアユニークキー演算ブロックをＤＶＤドライブ４が持つようにしたものである。

第３の実施形態では、メディアユニークキー演算ブロック４８がＤＶＤドライブ４に設けられているので、ＤＶＤメディア１から再生されたＭＫＢおよびメディアＩＤをホスト５へ転送することが不要となる。その結果、ＭＡＣ演算ブロック、計算されたＭＡＣ値の比較および比較出力で制御されるスイッチが不要となる。リボケーションもホスト５に依存することがなくなり、ＤＶＤメディア１とＤＶＤドライブ４だけで処理が完結するようになる。

ＤＶＤドライブ４に設けられたメディアユニークキー演算ブロック４８において、ＭＫＢ１２とメディアＩＤとデバイスキー４６とからメディアユニークキーが演算される。ＭＫＢ１２とデバイスキー４６とを使用してメディアキーが計算され、メディアＩＤ１１とメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキーをセキュアにホスト５に伝送するために、メディアユニークキーがＤＥＳエンクリプタ４９に供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト５のＤＥＳデクリプタ５９に供給され、バスキーを使用して復号される。

復号されたメディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められ、コンテンツキーを使用してＤＶＤメディア１から読み出された暗号化コンテンツが復号され、また、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

第９図は、第３の実施形態の処理の手順を示す。ＡＣＣのシークお

よびリード（ステップＳ４１）から残りのＭＫＢパックのリード（ステップＳ４８）までの処理は、第３図に示すものと同様であるので、この処理については、簡単に説明する。

ステップＳ４２では、認証が行われ、認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。ステップＳ４３において、ホスト５がＭＫＢ（メディアキーブロック）パック＃０の読み出しをＤＶＤドライブ４に要求し、ＤＶＤドライブ４がステップＳ４４においてＭＫＢパック＃０を読みに行き、ステップＳ４５において、パック＃０が読み出される。ステップＳ４６で、ＤＶＤドライブ４は、ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加したデータをホスト５へ転送する。ステップＳ４７およびＳ４８において、パック＃０以外の残りのＭＫＢパックの要求と、読み出し動作と、転送動作とがなされる。

ステップＳ４９において、ホスト５がメディアユニークキーを要求すると、ＤＶＤドライブ４が暗号化メディアユニークキーをホスト５に送る（ステップＳ５０）。メディアユニークキーが暗号化／復号モジュール５４に供給される。ステップＳ５１において、ホスト５が暗号化コンテンツを要求すると、ＤＶＤドライブ４が暗号化コンテンツをリードし（ステップＳ５２）、暗号化／復号モジュール５４によって暗号化コンテンツが復号され、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

第１０図は、この発明の第４の実施形態を示す。第４の実施形態では、第３の実施形態と同様に、メディアユニークキー演算ブロック４８をＤＶＤドライブ４が持ち、ホスト５がデバイスキー５６を持ち、ホスト５からＤＶＤドライブ４へデバイスキー５６をセキュアに転送

するものである。

第４の実施形態では、メディアユニークキー演算ブロック４８がＤＶＤドライブ４に設けられているので、ＤＶＤメディア１から再生されたＭＫＢおよびメディアＩＤをホスト５へ転送することが不要となる。その結果、ＭＡＣ演算ブロック、計算されたＭＡＣ値の比較および比較出力で制御されるスイッチが不要となる。

ホスト５のデバイスキー５６がＤＥＳエンクリプタ５９ｂに供給され、バスキーを鍵として暗号化される。暗号化デバイスキーがＤＶＤドライブ４のＤＥＳデクリプタ４９ｂに転送され、デバイスキーがＤＶＤドライブ４において復号される。復号されたデバイスキーがメディアユニークキー演算ブロック４８に入力される。

ＤＶＤドライブ４に設けられたメディアユニークキー演算ブロック４８において、ＭＫＢ１２とメディアＩＤとデバイスキー４６とからメディアユニークキーが演算される。すなわち、ＭＫＢ１２とデバイスキー４６とを使用してメディアキーが計算され、メディアＩＤ１１とメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキーがＤＥＳエンクリプタ４９ａに供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト５のＤＥＳデクリプタ５９ａに供給され、バスキーを使用して復号される。

復号されたメディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められ、コンテンツキーを使用してＤＶＤメディア１から読み出された暗号化コンテンツが復号され、また、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

第１１図は、第４の実施形態の処理の手順を示す。ＡＣＣのシーク

およびリード（ステップＳ６１）から残りのＭＫＢパックのリード（ステップＳ６８）までの処理は、第３図に示すものと同様であるので、この処理については、簡単に説明する。

ステップＳ６２では、認証が行われ、認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。次に、ステップＳ６３において、ホスト５がＭＫＢ（メディアキーブロック）パック＃０の読み出しをＤＶＤドライブ４に要求し、ＤＶＤドライブ４がステップＳ６４においてＭＫＢパック＃０を読みに行き、ステップＳ６５において、パック＃０が読み出される。ステップＳ６６で、ＤＶＤドライブ４は、ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加したデータをホスト５へ転送する。ステップＳ６７およびＳ６８において、パック＃０以外の残りのＭＫＢパックの要求と、読み出し動作と、転送動作とがなされる。

ステップＳ６９において、暗号化デバイスキーをホスト５がＤＶＤドライブ４に送る。ＤＶＤドライブ４において、メディアユニークキーが演算される。ステップＳ７０において、ホスト５がメディアユニークキーを要求すると、ＤＶＤドライブ４が暗号化メディアユニークキーをホスト５に送る（ステップＳ７１）。メディアユニークキーが暗号化／復号モジュール５４に供給される。ステップＳ７２において、ホスト５が暗号化コンテンツを要求すると、ＤＶＤドライブ４が暗号化コンテンツをリードし（ステップＳ７３）、暗号化／復号モジュール５４によって暗号化コンテンツが復号され、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

上述した第３および第４の実施形態では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算がドライブ４

内に実装されている。例えばＬＳＩ内にメディアユニークキー演算ブロック４８が実装される。ホスト５にインストールされるアプリケーションは、著作権保護技術に関するアルゴリズムの一部しか持たないで良い。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

第３の実施形態では、ＤＶＤメディア１を扱う正当なドライブとなるために、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

第１２図は、この発明の第５の実施形態を示す。上述した第１～第４の実施形態では、ＤＶＤの著作権保護技術であるＣＰＲＭに対してこの発明を適用したものである。第５の実施形態は、第２図に示す実際に運用されているＣＰＲＭのアーキテクチャを拡張した構成を有する。

第５の実施形態は、ホスト５のメディアユニークキー演算ブロック６１に対して、パラメータＡ６２が関与し、暗号化／復号モジュール６３に対して、パラメータＢ６４が関与するようにしたものである。パラメータＡ６２およびパラメータＢ６４は、固定値およびＤＶＤメディア１から読み出されたデータの何れであっても良い。

現行のＣＰＲＭでは、ＭＫＢとデバイスキーからメディアキーを計算し、メディアキーとメディアＩＤからメディアユニークキーを計算している。ＣＰＲＭを拡張したシステムにおいては、この計算の過程で、パラメータＡ６２が関与し、暗号化／復号モジュール６３では、コンテンツキーを計算する時に、パラメータＢ６４が関与する。第５の実施形態の処理の手順は、現行のＣＰＲＭと同様のものであり、そ

の図示については省略する。

第１３図は、この発明の第６の実施形態を示す。第６の実施形態は、実際に運用されているＣＰＲＭのアーキテクチャを拡張した構成を有し、デバイスキー４６と、パラメータＡ６２と、パラメータＢ６４とをＤＶＤドライブ４が持つようにしたものである。これらのデバイスキー４６、パラメータＡ６２およびパラメータＢ６４をセキュアにホスト５に伝送するために、ＤＥＳエンクリプタ６５でこれらの情報がバスキーで暗号化される。

比較５３においてＭＡＣ値が一致すると検出された場合、すなわち、完全性が確認できた場合にのみＯＮするスイッチＳＷ３を介して暗号化されたデータがＤＥＳデクリプタ６６に入力される。ＤＥＳデクリプタ６６には、バスキーが供給され、デバイスキー、パラメータＡ６２およびパラメータＢ６４が復号される。復号されたデバイスキーおよびパラメータＡがメディアユニークキー演算ブロック６１に供給され、ＭＫＢ１２とメディアＩＤとデバイスキー４６とパラメータＡとからメディアユニークキーが演算される。

メディアユニークキーおよびパラメータＢが暗号化／復号モジュール６３に供給され、これらのデータを使用してコンテンツキーが求められ、コンテンツキーを使用してコンテンツの暗号化／復号がなされる。

第１４図は、第６の実施形態の処理の手順を示す。ＡＣＣのシークおよびリード（ステップＳ８１）からメディアＩＤとｍ１をリターン（ステップＳ９２）までの処理は、現行のＣＰＲＭの処理と同様であるので、この処理については、簡単に説明する。ステップＳ８１では、ＡＣＣがシークされ、読み出され、ステップＳ８２において認証が成功すると、認証動作の度に異なる値となるセッションキーとしての

バスキーが生成される。

ステップＳ８３において、ホスト５がＭＫＢ（メディアキーブロック）パック＃０の読み出しをＤＶＤドライブ４に要求し、ＤＶＤドライブ４がステップＳ８４においてＭＫＢパック＃０を読みに行き、ステップＳ８５において、パック＃０が読み出される。ステップＳ８６で、ＤＶＤドライブ４は、ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加したデータ（モディファイドＭＫＢ）をホスト５へ戻す。ステップＳ８７およびＳ８８において、パック＃０以外の残りのＭＫＢパックの要求と、読み出し動作と、転送動作とがなされる。

ホスト５がメディアＩＤを要求し（ステップＳ８９）、ＤＶＤドライブ４がメディアＩＤを読みに行き（ステップＳ９０）、ステップＳ９１において、メディアＩＤが読み出される。ＤＶＤドライブ４は、メディアＩＤを読み出す際に、バスキーをパラメータとしてそのＭＡＣ値を計算し、ステップＳ９２において、読み出されたメディアＩＤに対してＭＡＣ値ｍ１を付加してホスト５へデータを転送する。

ホスト５では、ＤＶＤドライブ４から受け取ったＭＫＢ１２およびメディアＩＤ１１からバスキーをパラメータとして再度ＭＡＣ値を計算する。計算したＭＡＣ値とＤＶＤドライブ４から受け取ったＭＡＣ値とが一致したならば、正しいＭＫＢおよびメディアＩＤを受け取ったと判定して、スイッチＳＷ１およびスイッチＳＷ３をＯＮに設定して処理を先に進める。逆に両者が一致しなかったならば、ＭＫＢおよびメディアＩＤが改ざんされたものと判定して、スイッチＳＷ１およびスイッチＳＷ３をＯＦＦに設定して処理を停止する。

ステップＳ９３において、ホスト５がＤＶＤドライブ４に対してデバイスキーとパラメータＡとパラメータＢとを要求する。ＤＶＤドラ

イブ４は、デバイスキー４６とパラメータＡとパラメータＢとをＤＥＳエンクリプタ６５によって暗号化し、暗号化データをホスト５に送る（ステップＳ９４）。ホスト５は、バスキーを使用してＤＥＳデクリプタ６６によってデバイスキーを復号する。

ステップＳ９５において、ホスト５がＤＶＤドライブ４に対して暗号化コンテンツを要求し、ステップＳ９６において、ＤＶＤドライブ４が暗号化コンテンツを読み出し、ステップＳ９５において、読み出した暗号化コンテンツがホスト５に転送される。ホスト５のメディアユニークキー演算ブロック６１では、デバイスキー４６とＭＫＢ１２とメディアＩＤ１１とパラメータＡとによってメディアユニークキーが計算される。そして、メディアユニークキーが暗号化／復号モジュール６３に供給され、暗号化コンテンツが復号され、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

第１５図は、この発明の第７の実施形態を示す。第７の実施形態では、メディアユニークキー演算ブロック６７をＤＶＤドライブ４が持ち、ホスト５がデバイスキー５６とパラメータＡ６２とパラメータＢ６４とを持ち、ホスト５からＤＶＤドライブ４へデバイスキー５６およびパラメータＡ６２をセキュアに転送するものである。

第７の実施形態では、メディアユニークキー演算ブロック６７がＤＶＤドライブ４に設けられているので、ＤＶＤメディア１から再生されたＭＫＢおよびメディアＩＤをホスト５へ転送することが不要となる。その結果、ＭＡＣ演算ブロック、計算されたＭＡＣ値の比較および比較出力で制御されるスイッチが不要となる。

ホスト５のデバイスキー５６およびパラメータＡ６２がＤＥＳエンクリプタ６８に供給され、バスキーを鍵として暗号化される。暗号化データがＤＶＤドライブ４のＤＥＳデクリプタ６９に転送され、デバ

イスキーおよびパラメータＡがＤＶＤドライブ４において復号される。復号されたデバイスキーおよびパラメータＡがメディアユニークキー演算ブロック６７に入力される。

ＤＶＤドライブ４に設けられたメディアユニークキー演算ブロック６７において、ＭＫＢ１２とメディアＩＤとデバイスキー４６とパラメータＡとからメディアユニークキーが演算される。メディアユニークキーがＤＥＳエンクリプタ７０に供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト５のＤＥＳデクリプタ７１に供給され、バスキーを使用して復号される。

復号されたメディアユニークキーが暗号化／復号モジュール６３に供給され、暗号化タイトルキー１４、ＣＣＩ１５およびパラメータＡからコンテンツキーが求められる。コンテンツキーを使用してＤＶＤメディア１から読み出された暗号化コンテンツが復号され、また、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

第１６図は、第７の実施形態の処理の手順を示す。ＡＣＣのシークおよびリード（ステップＳ１０１）から残りのＭＫＢパックのリード（ステップＳ１０８）までの処理は、現行のＣＰＲＭの処理と同様であるので、この処理については、簡単に説明する。

ステップＳ１０２では、認証が行われ、認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。ステップＳ１０３において、ホスト５がＭＫＢ（メディアキーブロック）パック＃０の読み出しをＤＶＤドライブ４に要求し、ＤＶＤドライブ４がステップＳ１０４においてＭＫＢパック＃０を読みに行き、ステップＳ１０５において、パック＃０が読み出される。ステップＳ１０６で、ＤＶＤドライブ４は、ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を

付加したデータをホスト５へ転送する。ステップＳ１０７およびＳ１０８において、パック＃０以外の残りのＭＫＢパックの要求と、読み出し動作と、転送動作とがなされる。

ステップＳ１０９において、暗号化デバイスキーおよび暗号化パラメータをホスト５がＤＶＤドライブ４に送る。ステップＳ１１０において、ホスト５がメディアユニークキーを要求する。ＤＶＤドライブ４において、メディアユニークキーが演算される。ステップＳ１１１において、ＤＶＤドライブ４が暗号化メディアユニークキーをホスト５に送る。メディアユニークキーが暗号化／復号モジュール６３に供給される。ステップＳ１１２において、ホスト５が暗号化コンテンツを要求すると、ＤＶＤドライブ４が暗号化コンテンツをリードし（ステップＳ１１３）、暗号化／復号モジュール６３によって暗号化コンテンツが復号され、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

この発明の第８の実施形態について、第１７図を参照して説明する。第８の実施形態は、上述した第３の実施形態（第８図）と同様に、メディアユニークキーをドライブで生成するものである。第５の実施形態（第１２図）、第６の実施形態（第１３図）または第７の実施形態（第１５図）に示すように、コンテンツキーを生成する場合に関与するパラメータＢを使用するもの（ＣＰＲＭを拡張したシステム）である。

ＣＰＲＭを拡張したシステムにおいて、メディアユニークキーを演算するためのパラメータＡと、暗号化／復号のためのパラメータＢとが使用される。これらのパラメータＡ，Ｂがホスト側にある場合と、ドライブ側にある場合と、メディアに記録されており、ホストが読み出す場合との全てが可能である。パラメータＡ，Ｂをインターフェー

スを介して授受する場合には、暗号化がなされ、セキュアな伝送が必要とされる。

第１７図において、参照符号１０１が記録可能なメディアを示し、メディア１０１には、ＥＫＢ１１１、暗号化ディスクキーＥｍ（Ｋｄ）１１２、暗号化コンテンツ１１３、ディスクＩＤ１１４およびユニットキー生成用値Ｖｕ１１５が記録されている。第１７図では、省略しているが、暗号化コンテンツ１１３に関連してＣＣＩが記録されているのは、上述した第１～第７の実施形態例えば第３の実施形態と同様である。

第１７図中に記載されている鍵情報に関する用語を下記に説明する。

ＥＫＢ１１１は、各デバイスキーに対してメディアキーＫｍを配布するための鍵束である。既述の実施形態におけるメディアキーブロックＭＫＢに相当する。

メディアキーＫｍは、メディア毎に固有の鍵情報である。ＥＫＢの中にメディアキーが見つからない場合は、そのデバイスキーがリボークされたことを示す。

ディスクキーＫｄは、少なくともコンテンツ毎に異なる鍵情報である。コンテンツのマスターディスク毎に異ならせても良い。暗号化ディスクキーＥｍ（Ｋｄ）１１２は、メディアキーＫｍでディスクキーＫｄを暗号化した暗号化鍵で、メディア１０１に記録されている。暗号化ディスクキーＥｍ（Ｋｄ）１１２は、ドライブ１０４において、個々のメディア毎に異なるエンベディッドキーＫｅを生成するために使用される。第５～第７の実施形態におけるパラメータＡ（ドライブ４においてメディアユニークキーを生成するのに使用されるパラメータ）に相当する。

ユニットキー生成用値Ｖｕ１１５は、暗号化単位（暗号化ユニットと称する）ごとに定義することが可能なパラメータである。各暗号化ユニットは、複数のセクタデータから構成される。ユニットキー生成用値Ｖｕ１１５は、ホスト１０５において暗号化コンテンツ１１３を復号するユニットキーＫｕを生成するために使用される。第５～第７の実施形態におけるパラメータＢ（ホスト５において暗号化コンテンツ１３を暗号化／復号するために使用されるパラメータ）に相当する。

ディスクＩＤ１１４は、スタンパ毎に異なるＩＤである。第３の実施形態におけるメディアＩＤに相当する。

エンベディッドキーＫｅは、個々のメディア毎に異なる鍵情報であり、第３の実施形態におけるメディアユニークキーに相当する。

ドライブ１０４が持つデバイスキー１４６と、メディア１０１が持つＥＫＢ１１１とに基づいてメディアキーＫｍが得られる。メディアキーＫｍとメディア１０１が持つ暗号化ディスクキーＥｍ（Ｋｄ）１１２とに基づいてディスクキーＫｄが得られる。ディスクキーＫｄとディスクＩＤ１１４とに基づいてエンベディッドキーＫｅが得られる。

ユニットキーＫｕは、暗号化コンテンツ１１３を暗号化／復号する鍵であり、エンベディッドキーＫｅとユニットキー生成用値Ｖｕとに基づいて得られる。ユニットキーＫｕは、上述の実施形態におけるコンテンツキーに相当する。

上述した第８の実施形態の動作について処理の流れにしたがって説明する。

最初にＡＫＥ１４１および１５１による認証がなされる。認証が成功すると、バスキーが生成される。第１７図では省略されているが、

ＡＫＥ１４１および１５１の少なくとも一方に対して認証に関係するパラメータが供給されている。

ドライブ１０４では、メディア１０１からＥＫＢを読み出し、ドライブ１０４に供給する。メディア１０１からのＥＫＢとデバイスキー１４６がドライブ１０４のプロセスＥＫＢ１２２で演算され、メディアキーＫｍが算出される。演算結果が例えば０になるような場合では、デバイスキーがリボークされる。ドライブ１０４が有しているデバイスキー１４６は、例えば機種単位でドライブに与えられる固有の鍵である。

ドライブ１０４が暗号化ディスクキーＥｍ（Ｋｄ）をメディア１０１から読み出し、ＡＥＳ＿Ｄ１２３において、メディアキーＫｍによってディスクキーＫｄが復号される。ＡＥＳ(Advanced Encryption Standard)は、米国政府がＤＥＳに代わる新しい暗号化標準として採用した暗号化方法である。

さらに、ドライブ１０４は、メディア１０１からディスクＩＤ１１５を読み出し、ＡＥＳ＿Ｇ１４８において、ディスクＩＤとディスクキーＫｄを演算し、エンベディッドキーＫｅを得る。

ドライブ１０４とホスト１０５の認証が完了し、バスキーが得られているならば、ホスト１０５がドライブ１０４に対してエンベディッドキーＫｅの転送を要求する。

ドライブ１０４がインターフェース１０４ａを経由してホスト１０５に対してＫｅを転送する際に、ＡＥＳエンクリプタ１４９にてバスキーによりＫｅを暗号化する。ホスト１０５は、ＡＥＳデクリプタ１５９によって復号を行い、Ｋｅを得る。ＡＥＳエンクリプタ１４８およびＡＥＳデクリプタ１４９は、例えばＣＢＣ(Cipher Block Chaining)モードの処理を行う。

ホスト１０５は、コンテンツを暗号化ユニット単位で処理する。ホスト１０５は、読み出したい暗号化ユニットのユニットキー生成用値Ｖｕ１１５をドライブ１０４から読み出す。ＡＥＳ＿Ｇ１５８において、エンベディッドキーＫｅとユニットキー生成用値Ｖｕとからユニットキーが計算される。

ホスト１０５は、読み出したい暗号化コンテンツ１１３中の暗号化ユニットをセクタデータ単位で読み出す。ドライブ１０４は、ホスト１０５に対して読み出したセクタデータを転送する。セクタデータがホスト１０５の暗号化／復号モジュール１５４において、属する暗号化ユニットのユニットキーＫｕで復号される。

次に、第１８図を参照してこの発明の第９の実施形態について説明する。第９の実施形態は、ＲＯＭタイプのメディア１１０例えばＲＯＭディスクを再生する例である。

ＲＯＭタイプのメディア１１０には、予めコンテンツが記録されている。ホスト１０５では、暗号化の処理が不要となり、復号モジュール１６０が使用される。メディア１１０から読み出された暗号化コンテンツが復号モジュール１６０にて復号され、ＡＶコンテンツが得られる。

ＲＯＭタイプのメディア１１０の場合では、メディアキーＫｍおよびディスクキーＫｄがコンテンツ毎に固有の鍵情報である。各コンテンツは、１または複数の暗号化ユニットから構成される。

メディア１１０上にエンベディッドキー生成値Ｖｅが記録される。エンベディッドキー生成値Ｖｅは、ディスク製造工場でスタンパー（フォトレジストを現像したディスク原盤またはディスク原盤から最初に作成されたスタンパーを意味する）毎に、記録されたゼロでない値である。物理的ウォーターマークとして、通常のデータ記録とは、別

の手段でディスク上に記録される。

エンベディッドキーＫｅは、第３の実施形態におけるメディアユニークキーに相当する。エンベディッドキーＫｅを生成するためのエンベディッドキー生成値Ｖｅは、一種のメディアＩＤである。

第９の実施形態も、上述した第８の実施形態と同様の処理を行う。最初にＡＫＥ１４１および１５１による認証がなされ、バスキーが生成される。読み出されたＥＫＢとデバイスキー１４６がドライブ１０４のプロセスＥＫＢ１２２で演算され、メディアキーＫｍが算出とリボーク処理がなされる。そして、ＡＥＳ＿Ｄ１２３において、メディアキーＫｍによってディスクキーＫｄが復号される。さらに、ＡＥＳ＿Ｇ１４８において、エンベディッドキーＫｅが得られる。

ＡＥＳエンクリプタ１４９にてバスキーによりＫｅが暗号化される。ホスト１０５は、ＡＥＳデクリプタ１５９によって復号を行い、Ｋｅを得る。

ホスト１０５は、読み出したい暗号化ユニットのユニットキー生成用値Ｖｕ１１５をドライブ１０４から読み出し、ＡＥＳ＿Ｇ１５８において、ユニットキーＫｕが計算される。

ホスト１０５が要求した暗号化ユニットのセクタデータがホスト１０５の復号モジュール１６０において、属する暗号化ユニットのユニットキーＫｕで復号される。

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーが記録再生装置内に実装されているので、ＤＶＤ処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報を持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著

作権保護技術の安全性を確保することができる。

電子機器またはアプリケーションソフトウェア固有の情報としてのデバイスキーを記録再生装置とデータ処理装置が分けて持つことによって、記録再生装置およびアプリケーションソフトウェアの両方について、リボーク処理を行うことが可能となる。

この発明では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算が記録再生装置内に実装されている。したがって、データ処理装置のアプリケーションソフトウェアは、著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばデバイスキーを二つに分割し、ドライブおよびホストが各デバイスキーを持つことも可能である。メディアユニークキー演算ブロックをドライブが持つ構成も可能である。

暗号化コンテンツををインターフェースを介して授受する場合に、暗号化を行い、セキュアな伝送を行っても良い。ＡＫＥに対して認証に関係するパラメータを供給するが、例えば排除すべきもののリストまたは排除すべきでないもののリストを供給するようにしても良い。

産業上の利用可能性

また、上述した説明においては、著作権保護技術としてＣＰＲＭおよびＣＰＲＭを拡張した例を挙げたが、ＣＰＲＭ以外の著作権保護技術に対してもこの発明を適用することができる。ＰＣベースのシステ

ムに対してこの発明が適用されているが、ＰＣとドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

請求の範囲

1． 記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報が格納される格納部と、

上記記録媒体固有の第1の情報と上記格納部に格納された第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

を有する記録再生装置。

2． 請求の範囲1において、

上記第2の情報の一部が上記格納部に格納され、上記データ処理装置に格納された他の部分と合成されて上記第2の情報が形成されるようにした記録再生装置。

3． 請求の範囲1において、

少なくとも上記格納部に格納された第2の情報と上記記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記データ処理装置に対して、上記接続部が上記格納部に格納された第2の情報を送る記録再生装置。

4． 請求の範囲3において、

上記第2の情報を暗号化して送る記録再生装置。

5． 請求の範囲1において、

上記格納部に格納された第２の情報と上記記録媒体固有の第１の情報とを用いて、当該格納された第２の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置。

６．　記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第２の情報が格納される格納部と、

上記記録媒体固有の第１の情報と上記格納部に格納された第２の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

少なくとも上記接続部を介して上記データ処理装置から送られ、上記格納部に格納された第２の情報と、上記記録媒体固有の第１の情報とを用いて、当該格納された第２の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置。

７．　請求の範囲６において、

暗号化された上記第２の情報を復号する復号手段を有する記録再生装置。

８．　正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第２の情報を有するとともに、記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録

されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

上記接続部を介して上記記録再生装置から送られた、上記記録媒体固有の第1の情報と上記電子機器またはアプリケーションソフトウェア固有の第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部と

を有するデータ処理装置。

9．　請求の範囲8において、

上記第2の情報の一部が上記格納部に格納され、上記記録再生装置に格納された他の部分と合成されて上記第2の情報が形成されるようにしたデータ処理装置。

10．　請求の範囲8において、

上記接続部を介して上記記録再生装置から送られた上記第2の情報と、上記記録媒体固有の第1の情報とを用いて、上記第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有するデータ処理装置。

11．　請求の範囲10において、

暗号化された上記第2の情報を復号する復号手段を有するデータ処理装置。

12．　請求の範囲8において、

少なくとも上記記録再生装置に格納された第2の情報と、上記記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記記録再生装置

と接続するデータ処理装置。

１３．　正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第２の情報を有する格納部と、

記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

上記記録媒体固有の第１の情報と上記格納部に格納された第２の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部とを有し、

上記格納部に格納された第２の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記記録再生装置に対して、上記格納部に格納された第２の情報を送るデータ処理装置。

１４．　請求の範囲１３において、

上記第２の情報を暗号化して送るデータ処理装置。

１５．　記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方が可能であると共に、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第２の情報を有する記録再生装置と、

少なくとも格納された上記第２の情報と、上記記録媒体固有の第１の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と

を有する記録再生処理システム。

１６．　請求の範囲１５において、

上記データ処理装置が上記記録媒体固有の第１の情報と格納された上記第２の情報を用いて、当該格納された第２の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生処理システム。

１７．　請求の範囲１５において、

上記記録再生装置が上記記録媒体固有の第１の情報と格納された上記第２の情報を用いて、当該格納された第２の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生処理システム。

１８．　正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報として格納された第２の情報を有するとともに、記録媒体固有の第１の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と、

格納された上記第２の情報と、上記記録媒体固有の第１の情報とに基づいて生成された鍵を用いてデータの暗号化、または暗号化されたデータの復号が可能なデータ処理装置とからなり、

格納された上記第２の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記記録再生装置に対して、上記データ処理装置が上記格納部に格納された第２の情報を送る記録再生処理システム。

１９．　不正な電子機器を無効化するための第１の情報と、コンテンツ毎に異なる第２の情報と、暗号化単位毎に定義可能な第３の情報と

、スタンパ毎に異なる識別データとが記録された記録媒体へ暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第４の情報が格納される格納部と、

上記第１の情報と上記第４の情報とから当該格納された第４の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であるかを判定するリボーク処理部と、

上記リボーク処理部で上記第４の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であると判定された場合に、上記第１の情報、上記第４の情報、上記第２の情報および上記識別データから、個々の記録媒体毎に固有の中間鍵情報を求める演算部と有する記録再生装置。

２０．　請求の範囲１９において、

上記中間鍵情報に基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う認証部と、

上記認証が成立した場合に形成されるバスキーによって上記中間鍵情報を暗号化して上記データ処理装置に送出する中間鍵情報暗号化部とを有する記録再生装置。

２１．　正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第４の情報を有するとともに、不正な電子機器を無効化するための第１の情報と、コンテンツ毎に異なる第２の情報と、暗号化単位毎に定義可能な第３の情報と、スタンパ毎に異なる識別データとが記録され

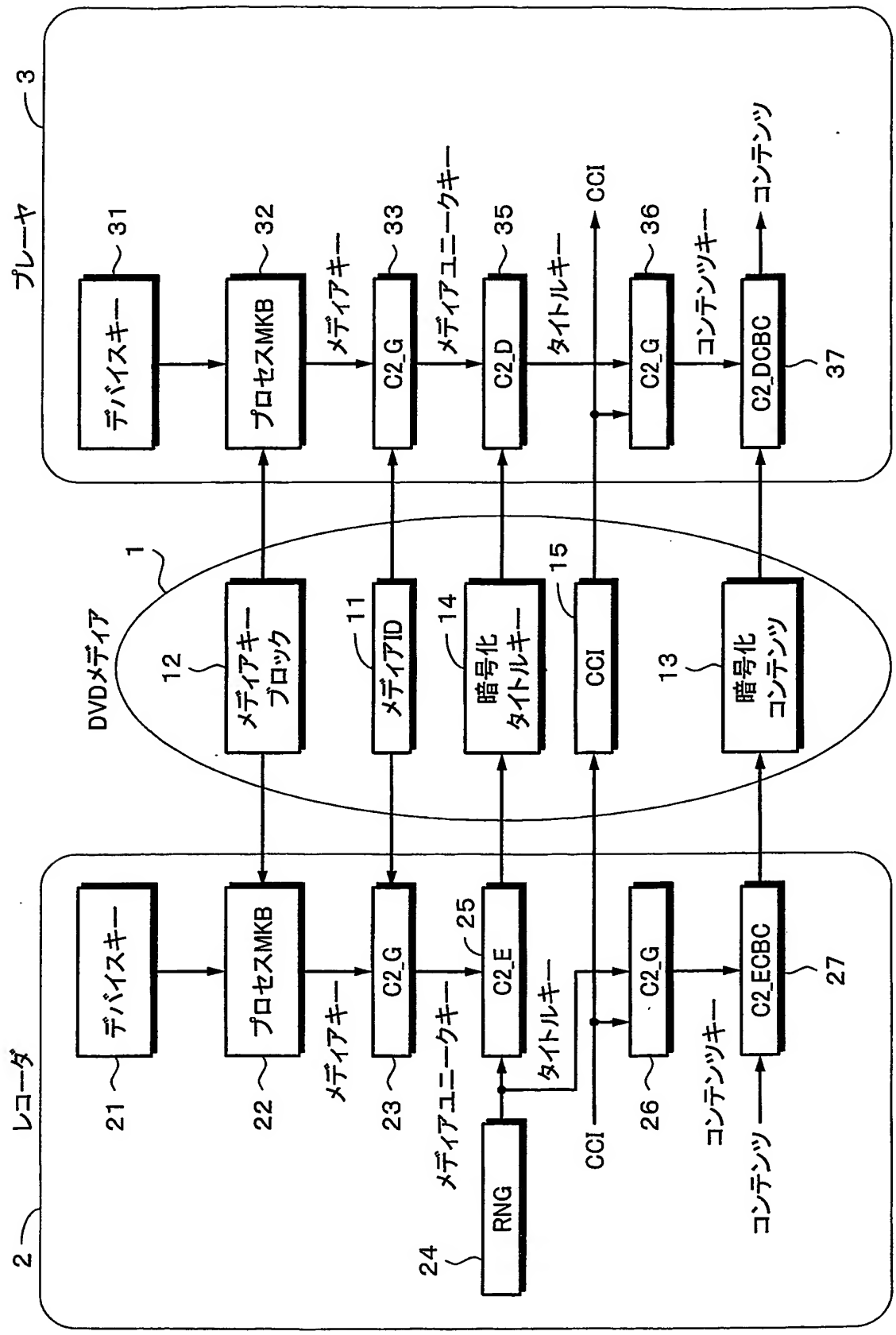
た記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置との認証を行う認証部と、

上記記録再生装置から、上記認証が成立した場合に形成されるバスキーによって暗号化された、上記第1の情報、上記第4の情報、上記第2の情報および上記識別データから生成された個々の記録媒体毎に固有の中間鍵情報を受け取り、当該中間鍵情報を復号する鍵情報復号部と、

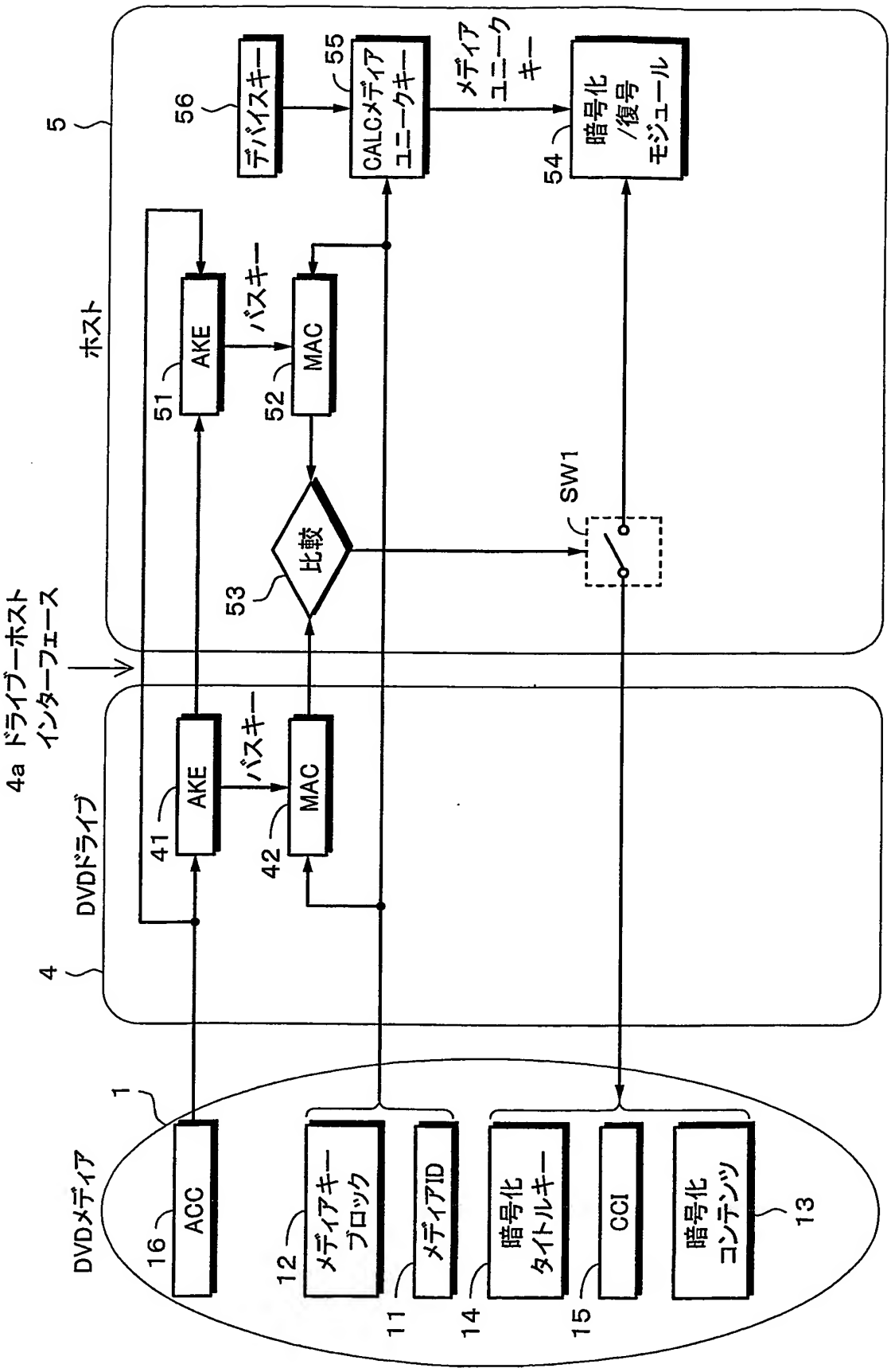
上記記録再生装置から受け取った上記第3の情報と、復号された上記中間鍵情報から暗号化鍵を生成する暗号化鍵生成部と、

上記暗号化鍵による暗号化と上記暗号化鍵による復号との少なくとも一方を行う暗号化復号部とを有するデータ処理装置。

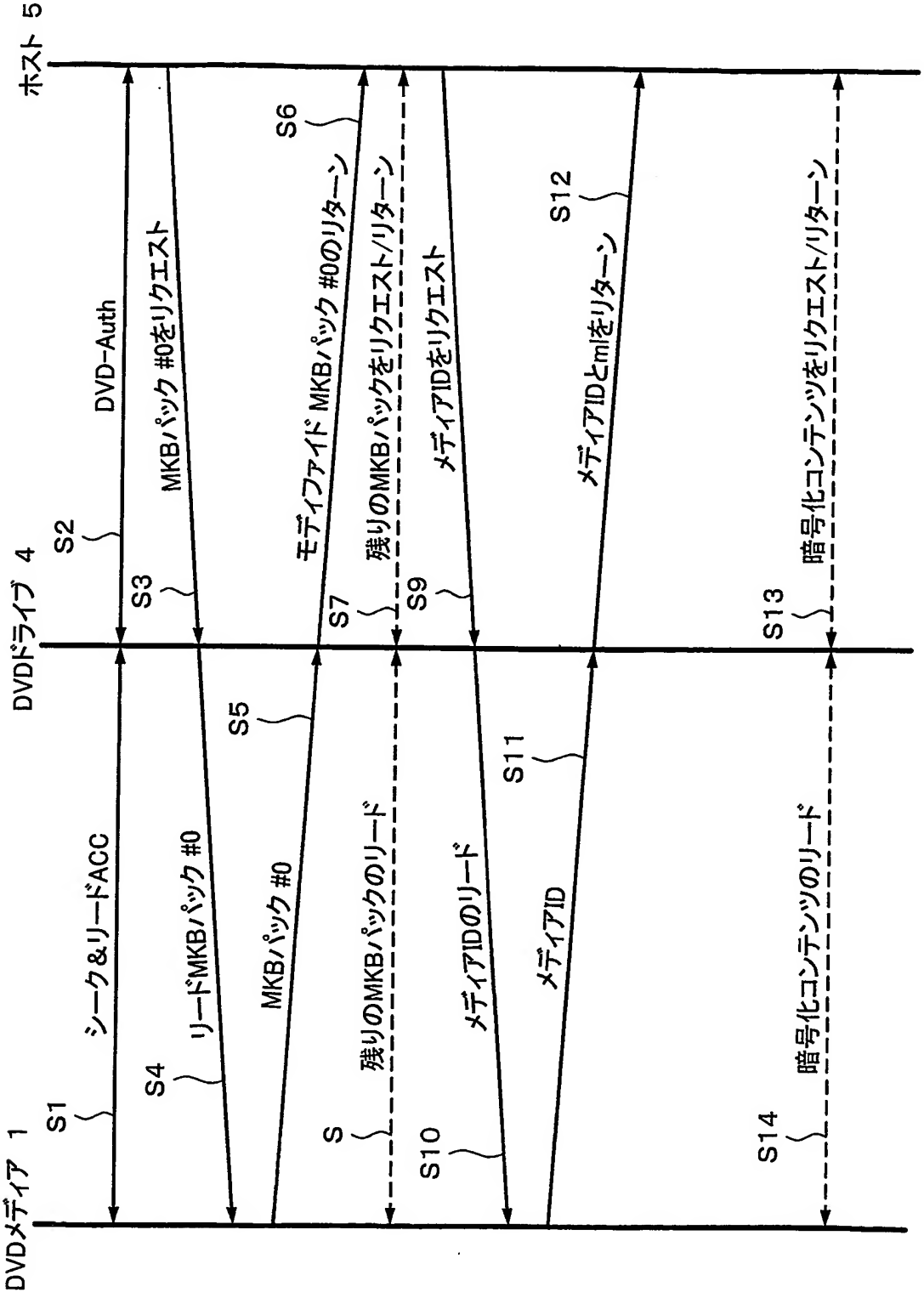
第１図


プレーヤ
3
デバイスキー
31
プロセスMKB
32
メディアキー
C2_G
33
メディアユニークキー
C2_D
35
タイトルキー
CCI
C2_G
36
コンテンツキー
C2_DCBC
37
コンテンツ
DVDメディア
1
メディアキーブロック
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
レコーダ
2
デバイスキー
21
プロセスMKB
22
メディアキー
C2_G
23
メディアユニークキー
C2_E
25
タイトルキー
CCI
C2_G
26
コンテンツキー
C2_ECBC
27
コンテンツ
RNG
24

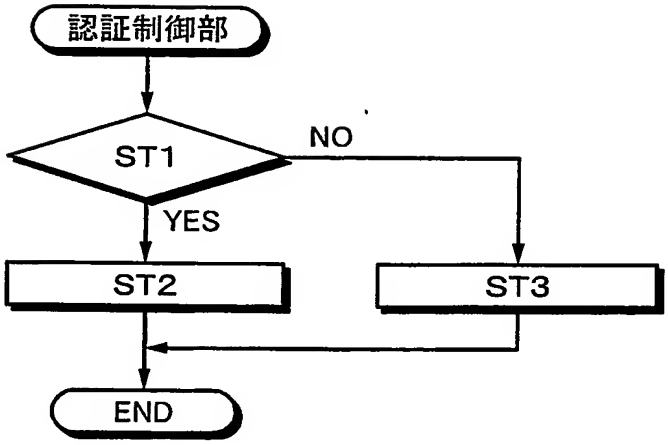
第２図


DVDメディア
1
ACC
16
メディアキーブロック
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
4
DVDドライブ
AKE
41
バスキー
MAC
42
4a ドライブーホストインターフェース
5
ホスト
AKE
51
バスキー
MAC
52
比較
53
SW1
デバイスキー
56
CALCメディアユニークキー
55
メディアユニークキー
暗号化/復号モジュール
54

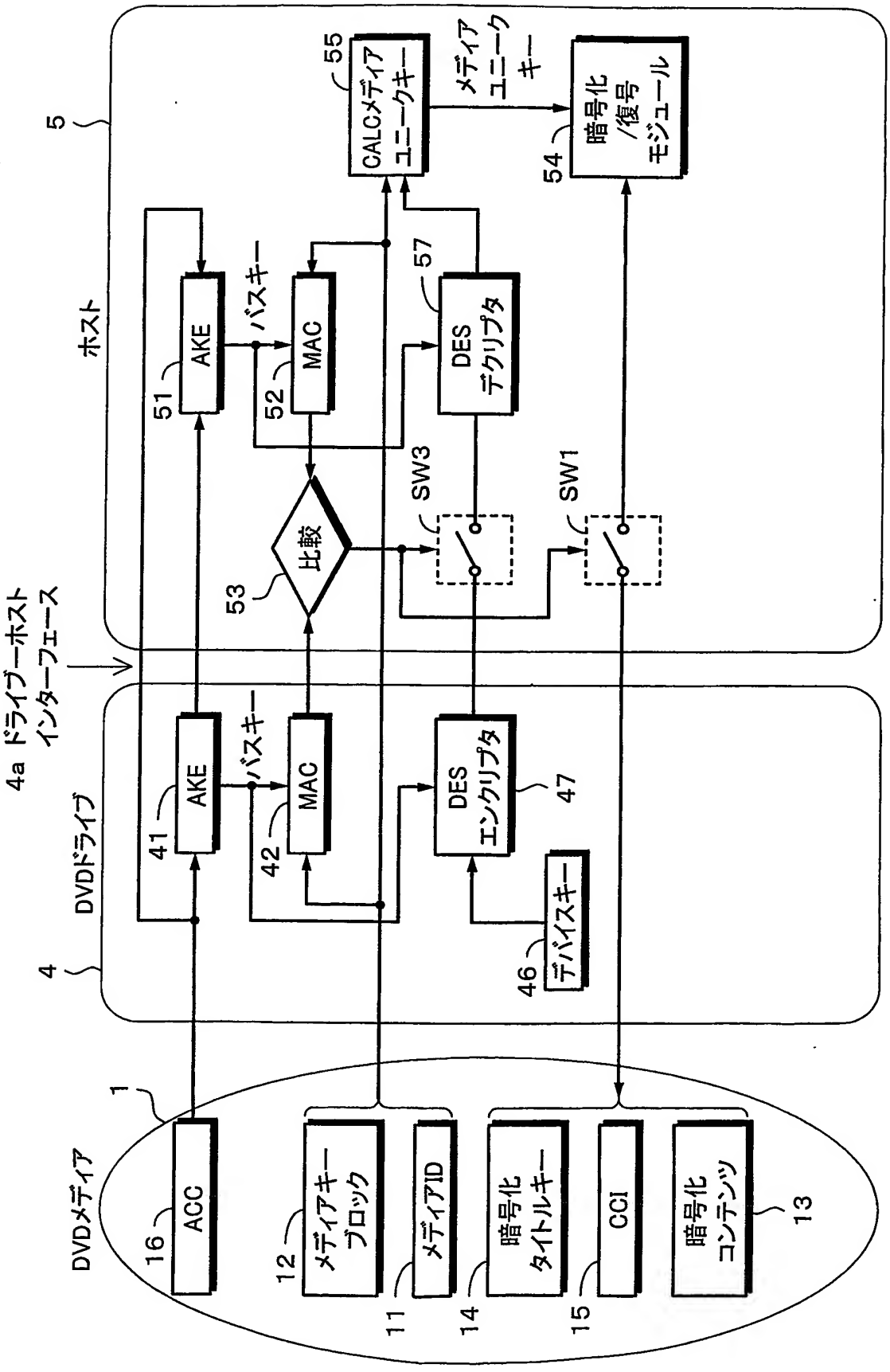
第３図


ホスト 5
DVDドライブ 4
DVDメディア 1
S1
シーク&リードACC
S2
DVD-Auth
S3
MKBパック #0をリクエスト
S4
リードMKBパック #0
S5
MKBパック #0
S6
モディファイド MKBパック #0のリターン
S7
S
残りのMKBパックのリード
残りのMKBパックをリクエスト/リターン
S9
メディアIDをリクエスト
S10
メディアIDのリード
S11
メディアID
S12
メディアIDとmlをリターン
S13
暗号化コンテンツをリクエスト/リターン
S14
暗号化コンテンツのリード

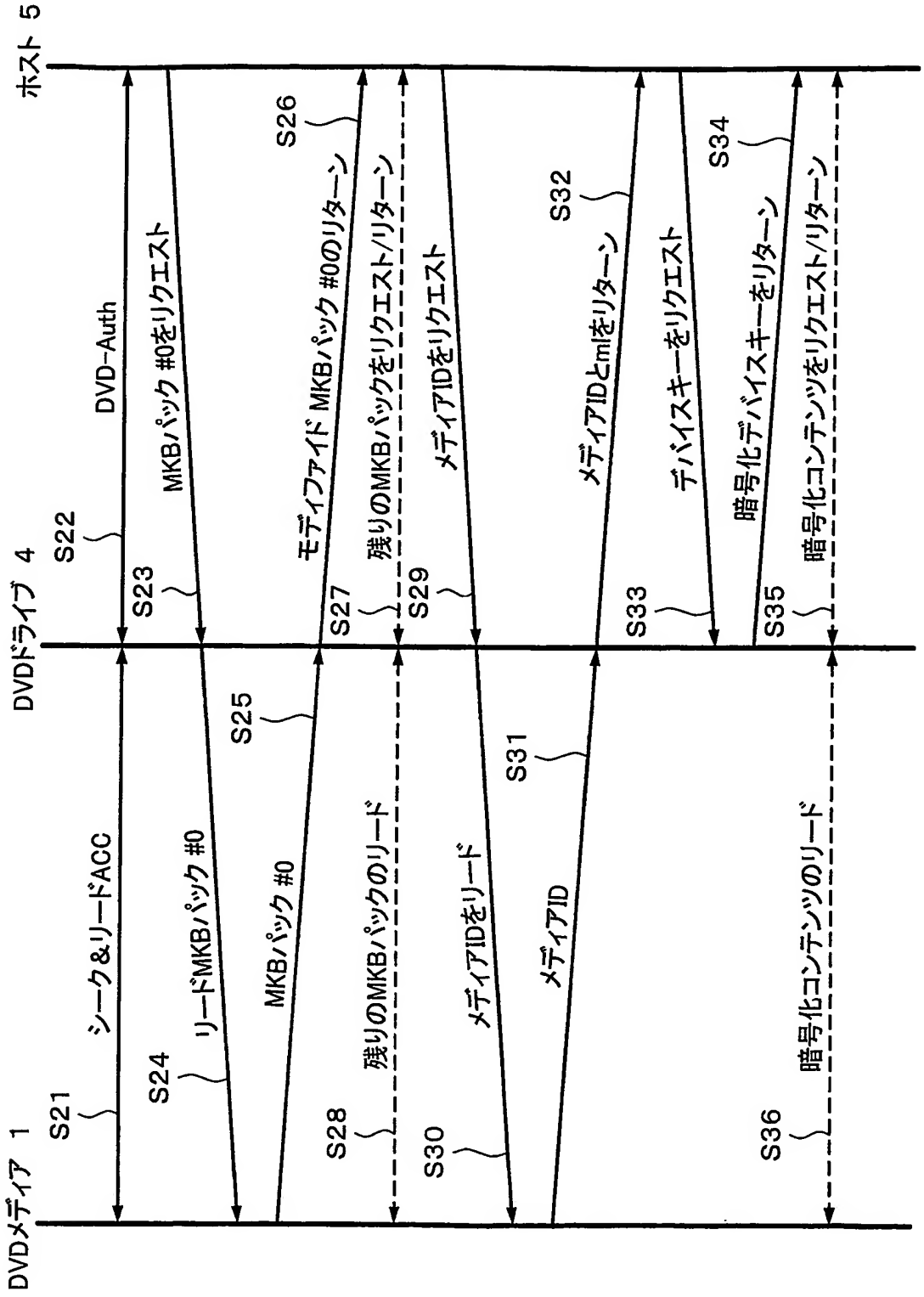
第４図



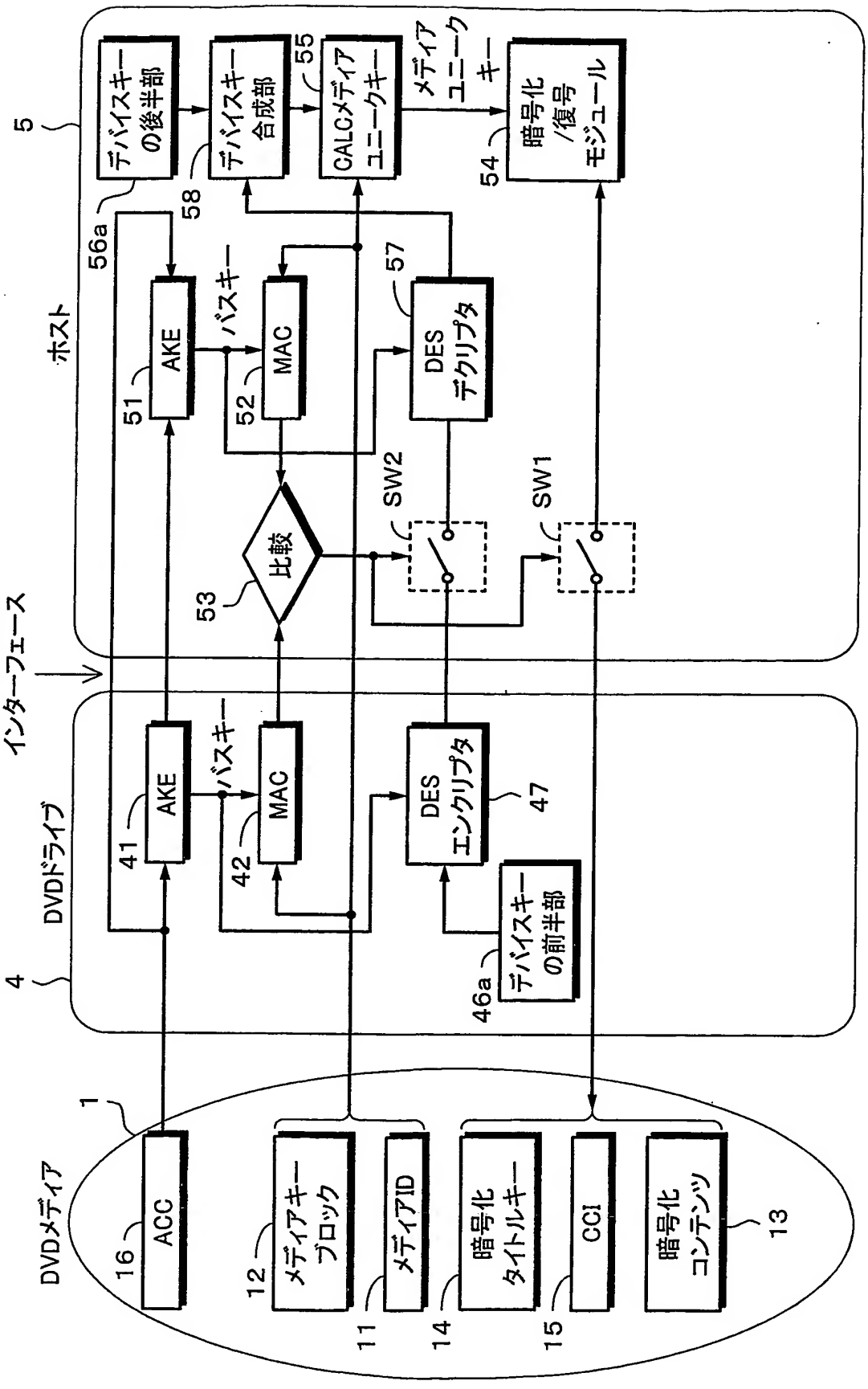
第5図


5
ホスト
4a ドライブーホスト
インターフェース
4
DVDドライブ
1
DVDメディア
55
CALCメディア
ユニークキー
メディア
ユニーク
キー
54
暗号化
/復号
モジュール
51
AKE
バスキー
52
MAC
57
DES
デクリプタ
SW3
SW1
53
比較
41
AKE
バスキー
42
MAC
DES
エンクリプタ
47
46
デバイスキー
16
ACC
12
メディアキー
ブロック
11
メディアID
14
暗号化
タイトルキー
15
CCI
暗号化
コンテンツ
13

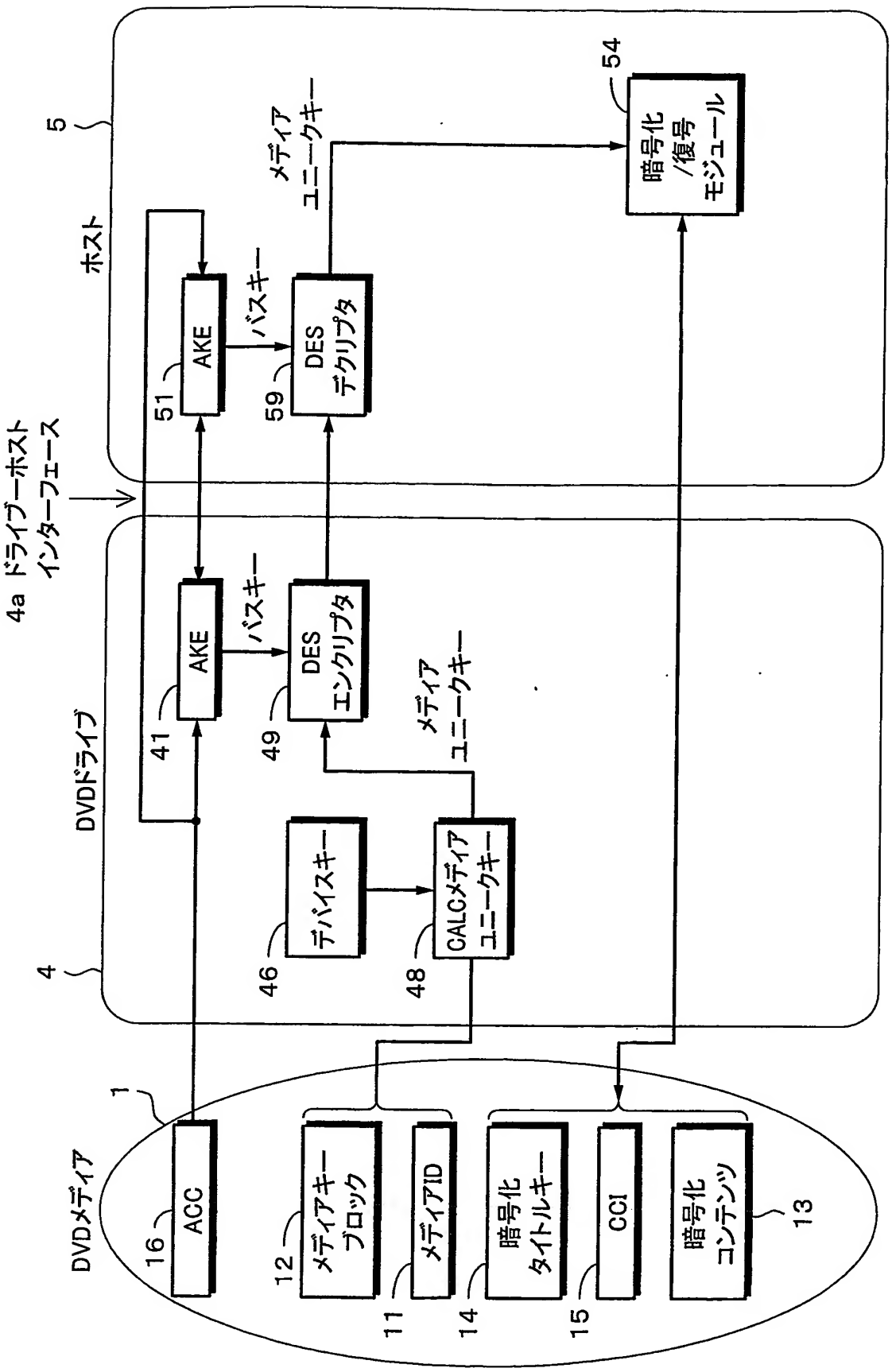
第6図


ホスト 5
DVDドライブ 4
DVDメディア 1
DVD-Auth
S22
S23
S21
シーク&リードACC
MKBパック #0をリクエスト
S24
リードMKBパック #0
S25
MKBパック #0
S26
モディファイド MKBパック #0のリターン
S27
S28
残りのMKBパックのリード
残りのMKBパックをリクエスト/リターン
S29
S30
メディアIDをリード
メディアIDをリクエスト
S31
メディアID
S32
メディアIDとmlをリターン
S33
デバイスキーをリクエスト
S34
暗号化デバイスキーをリターン
S35
S36
暗号化コンテンツのリード
暗号化コンテンツをリクエスト/リターン

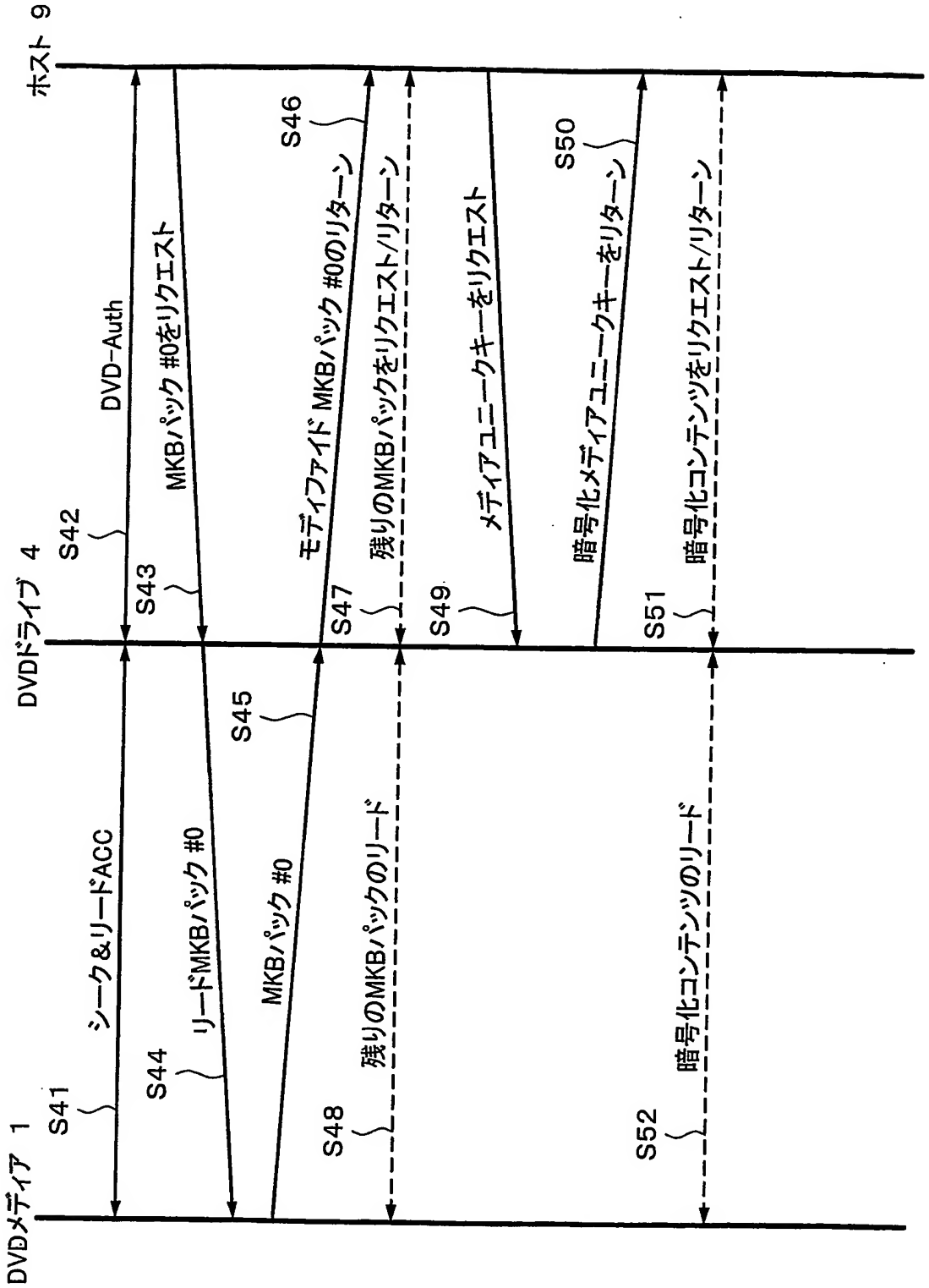
第７図


DVDメディア
1
ACC
16
メディアキーブロック
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
4
DVDドライブ
4a ドライブーホストインターフェース
AKE
41
バスキー
MAC
42
DES エンクリプタ
47
デバイスキーの前半部
46a
5
ホスト
AKE
51
バスキー
MAC
52
比較
53
DES デクリプタ
57
SW2
SW1
デバイスキーの後半部
56a
デバイスキー合成部
58
CALCメディアユニークキー
55
メディアユニークキー
暗号化/復号モジュール
54

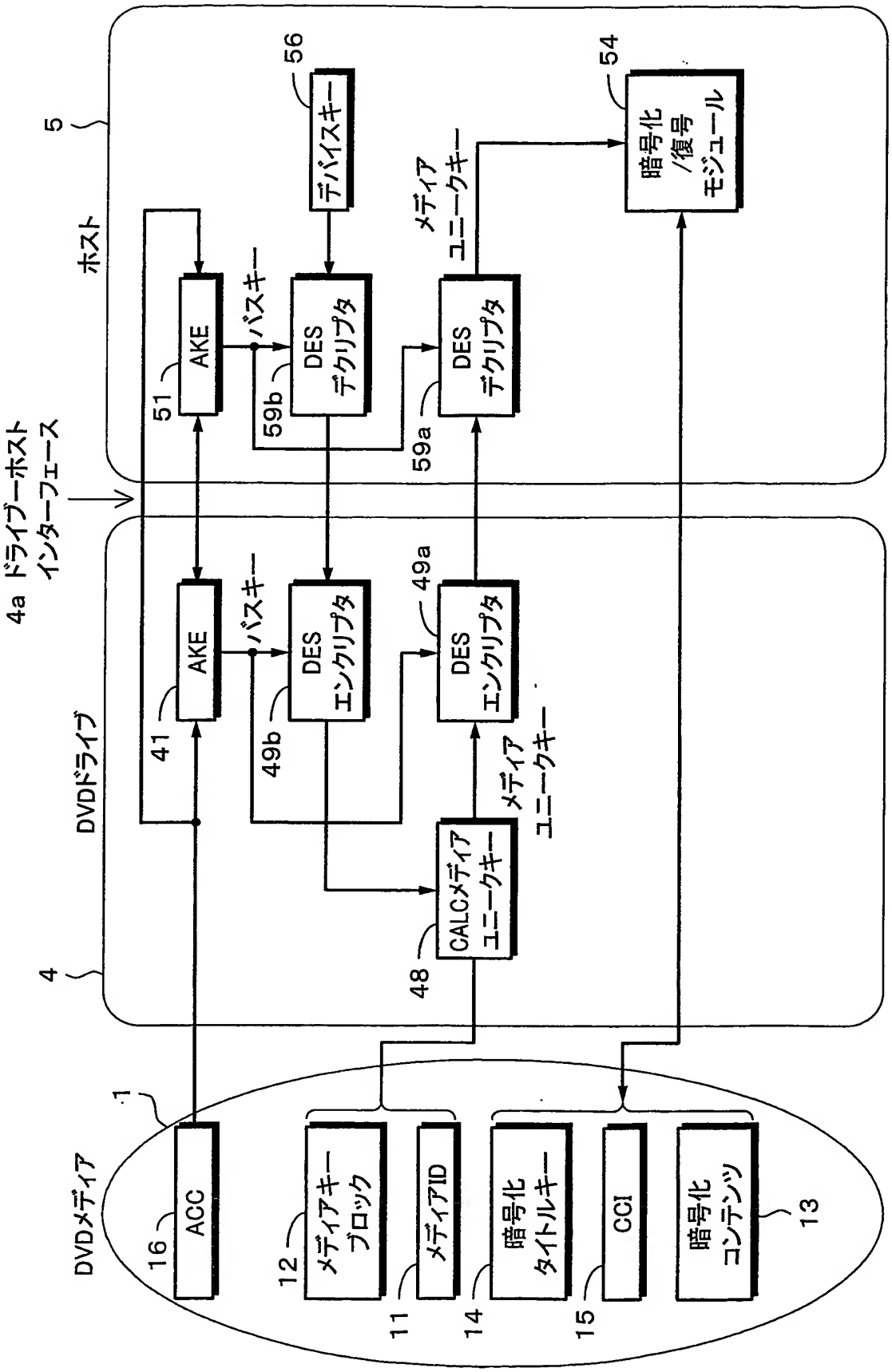
第８図


DVDメディア
1
ACC
16
メディアキーブロック
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
DVDドライブ
4
AKE
41
バスキー
DES エンクリプタ
49
デバイスキー
46
CALCメディアユニークキー
48
メディアユニークキー
4a ドライブーホストインターフェース
ホスト
5
AKE
51
バスキー
DES デクリプタ
59
メディアユニークキー
暗号化/復号モジュール
54

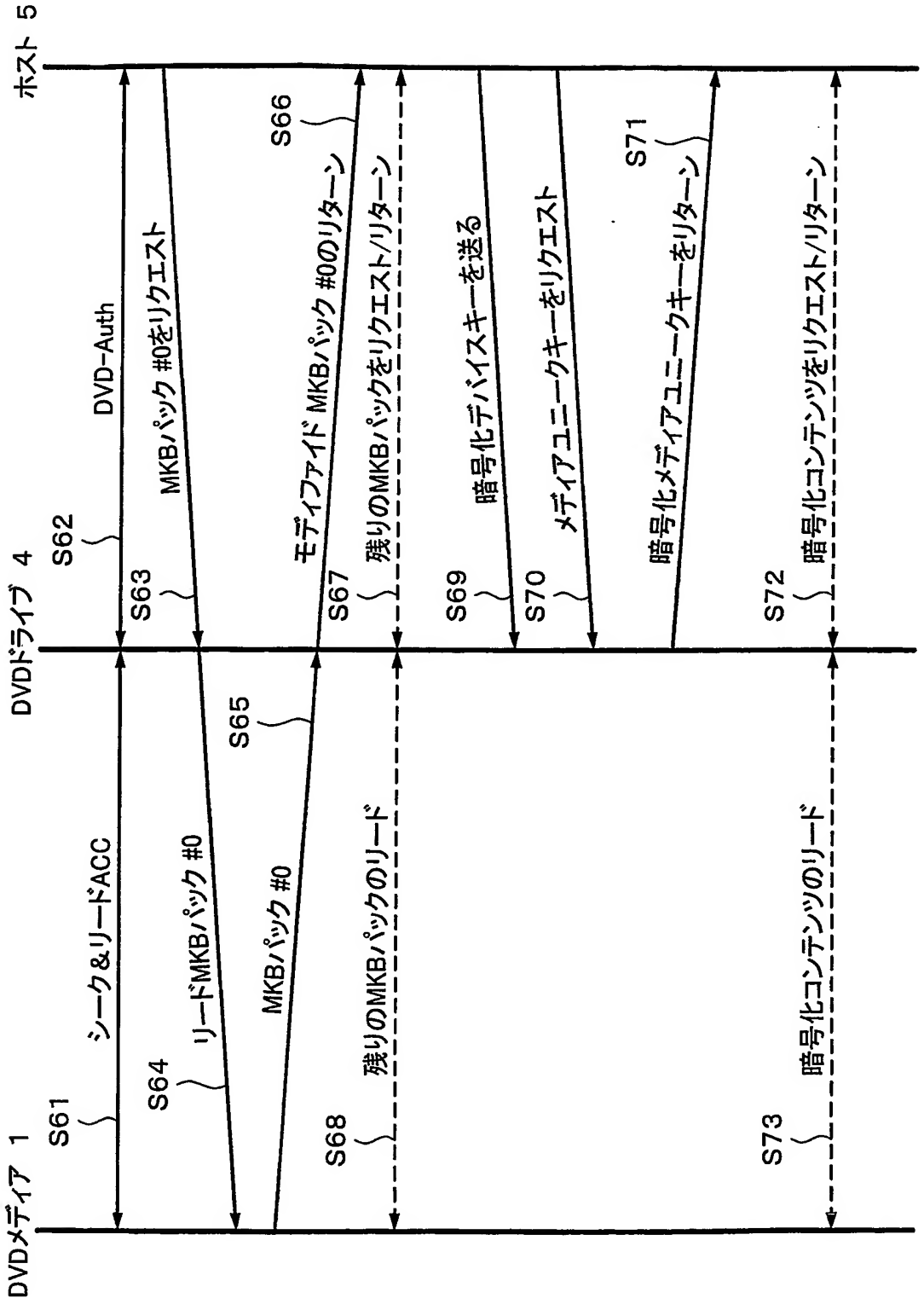
第9図


ホスト 9
DVDドライブ 4
DVDメディア 1
S41
シーク&リードACC
S42
DVD-Auth
S43
MKBパック #0をリクエスト
S44
リードMKBパック #0
S45
MKBパック #0
S46
モディファイド MKBパック #0のリターン
S47
残りのMKBパックをリクエスト/リターン
S48
残りのMKBパックのリード
S49
メディアユニークキーをリクエスト
S50
暗号化メディアユニークキーをリターン
S51
暗号化コンテンツをリクエスト/リターン
S52
暗号化コンテンツのリード

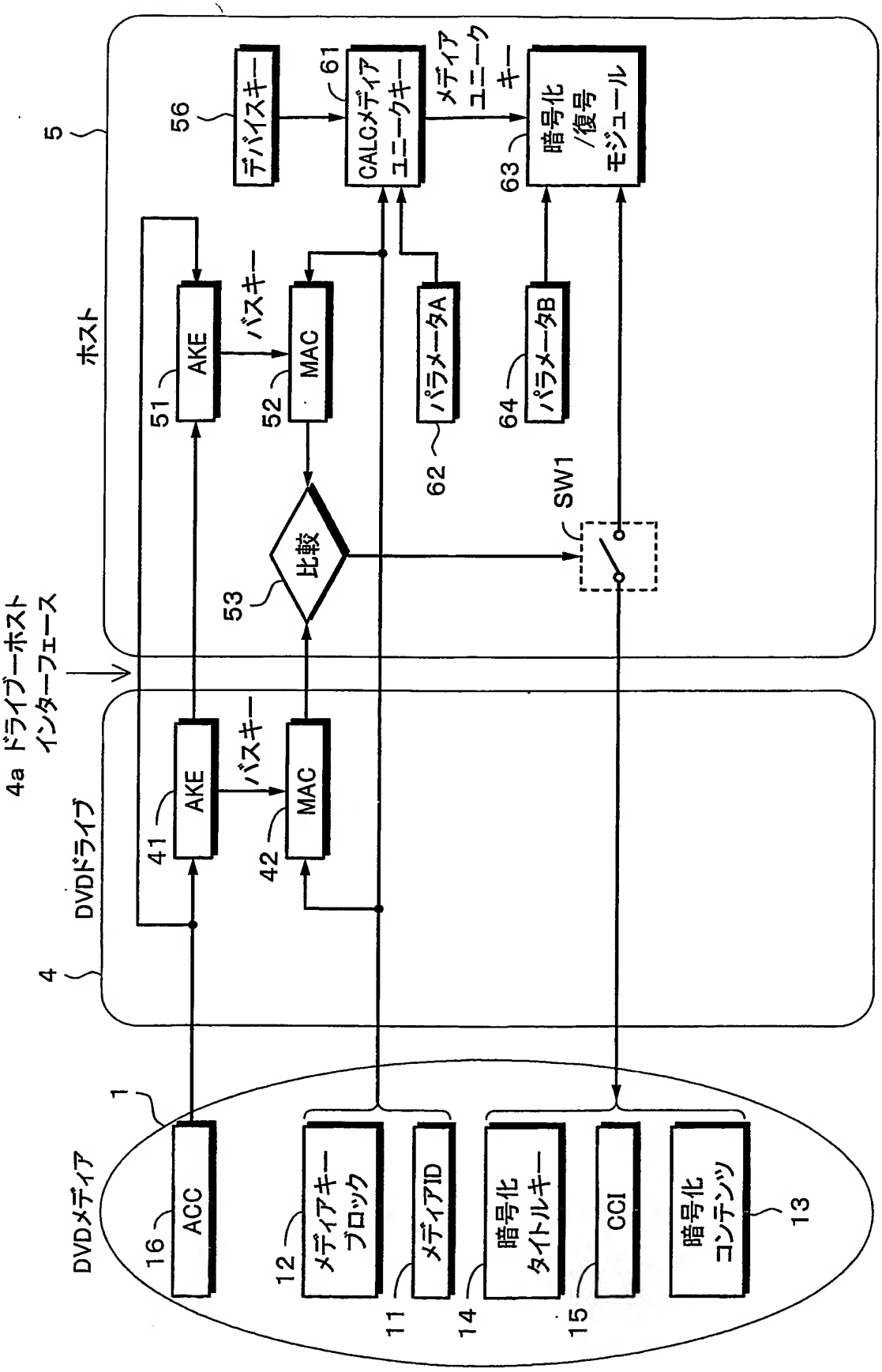
第１０図


5
ホスト
56
デバイスキー
54
暗号化
/復号
モジュール
メディア
ユニークキー
51
AKE
バスキー
59b
DES
デクリプタ
59a
DES
デクリプタ
4a ドライブーホスト
インターフェース
DVDドライブ
41
AKE
バスキー
49b
DES
エンクリプタ
49a
DES
エンクリプタ
メディア
ユニークキー
4
48
CALCメディア
ユニークキー
1
DVDメディア
16
ACC
12
メディアキー
ブロック
11
メディアID
14
暗号化
タイトルキー
15
CCI
暗号化
コンテンツ
13

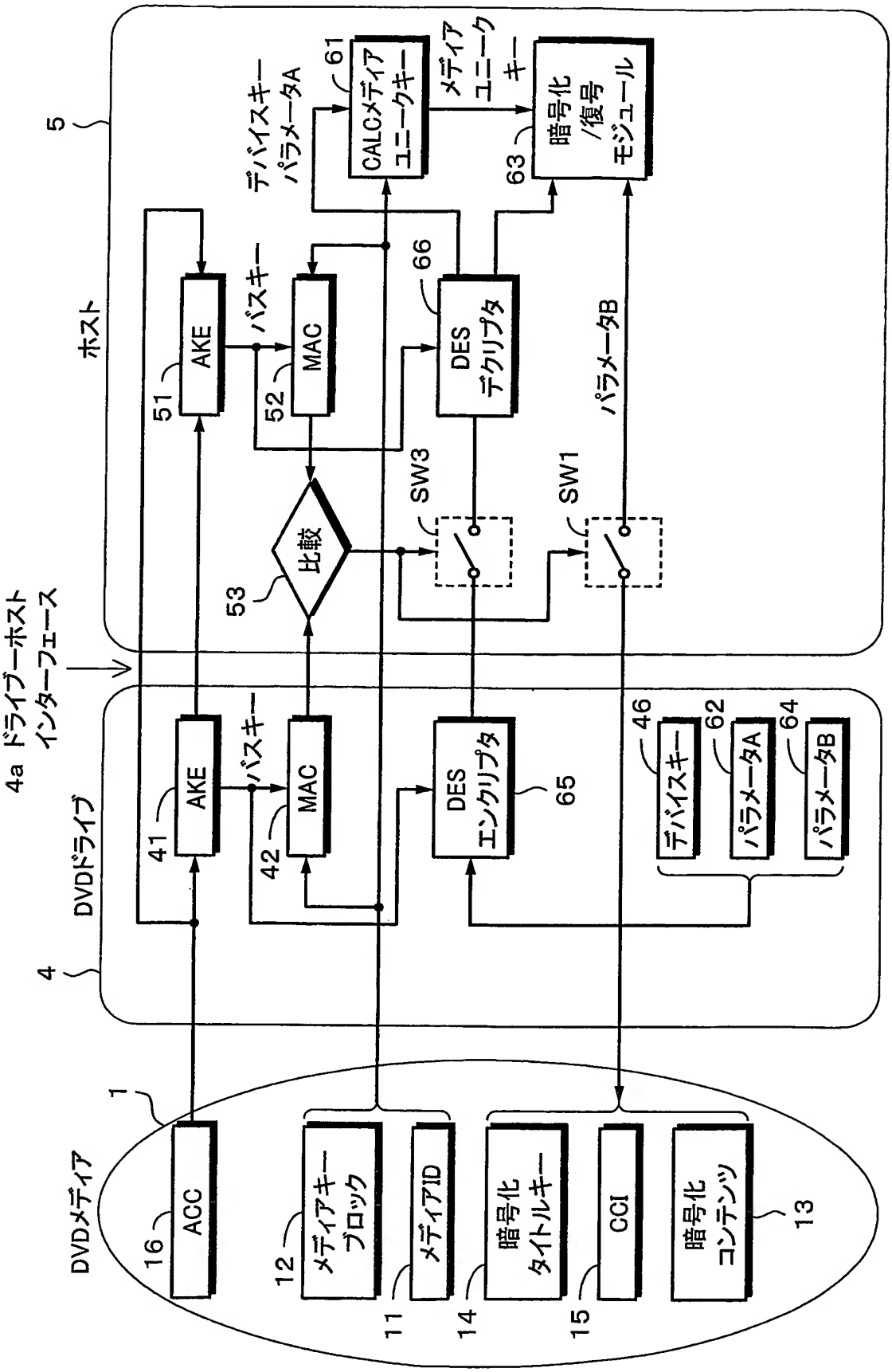
第１１図


ホスト 5
DVDドライブ 4
DVDメディア 1
S61
シーク&リードACC
S62
DVD-Auth
S63
MKBパック #0をリクエスト
S64
リードMKBパック #0
S65
MKBパック #0
S66
モディファイド MKBパック #0のリターン
S67
残りのMKBパックをリクエスト/リターン
S68
残りのMKBパックのリード
S69
暗号化デバイスキーを送る
S70
メディアユニークキーをリクエスト
S71
暗号化メディアユニークキーをリターン
S72
暗号化コンテンツをリクエスト/リターン
S73
暗号化コンテンツのリード

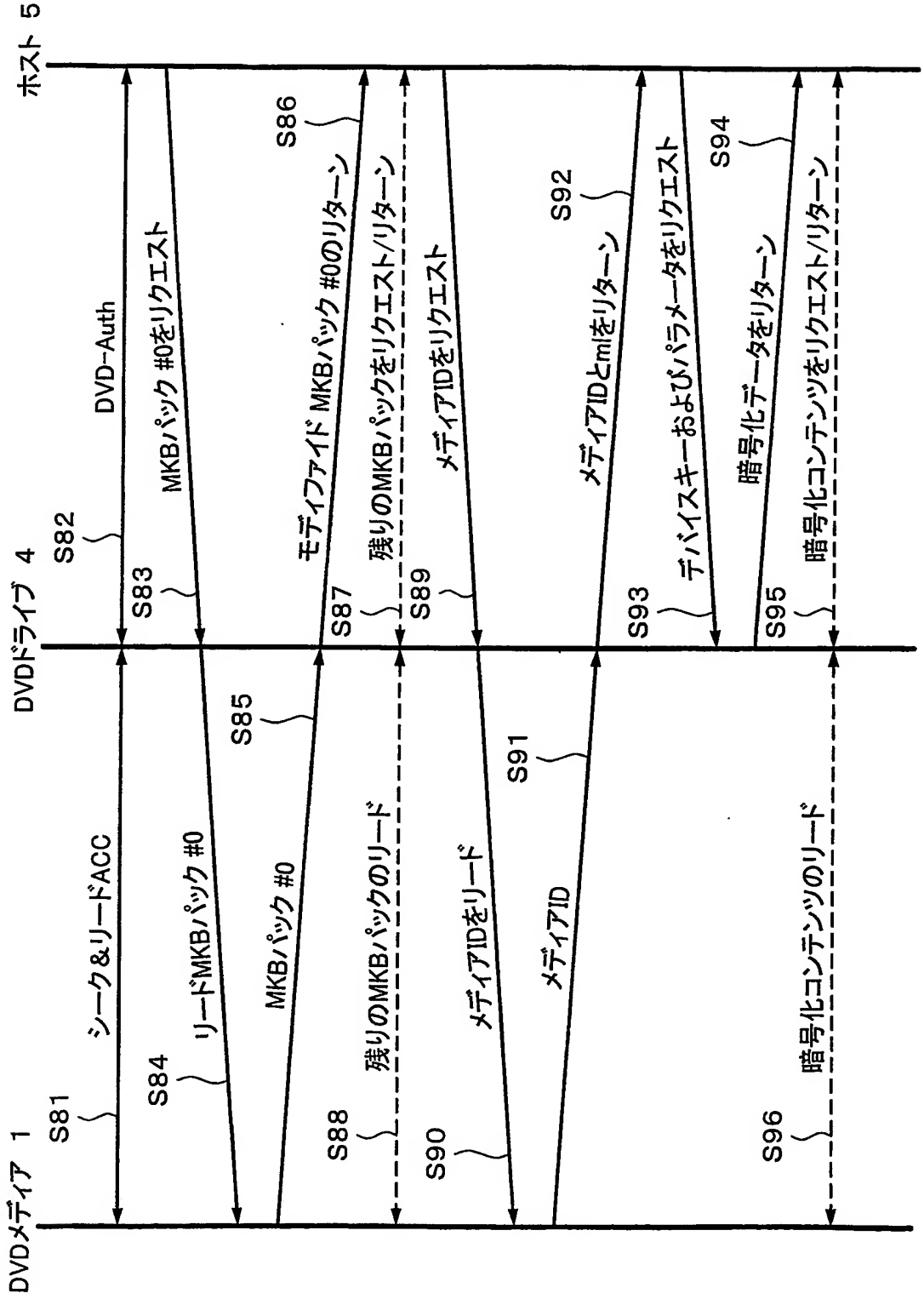
第１２図


5
ホスト
56
デバイスキー
61
CALCメディア
ユニークキー
メディア
ユニーク
キー
63
暗号化
/復号
モジュール
AKE
51
バスキー
MAC
52
パラメータA
62
パラメータB
64
SW1
比較
53
4a ドライブーホスト
インターフェース
4
DVDドライブ
41
AKE
バスキー
42
MAC
1
DVDメディア
16
ACC
12
メディアキー
ブロック
11
メディアID
14
暗号化
タイトルキー
15
CCI
暗号化
コンテンツ
13

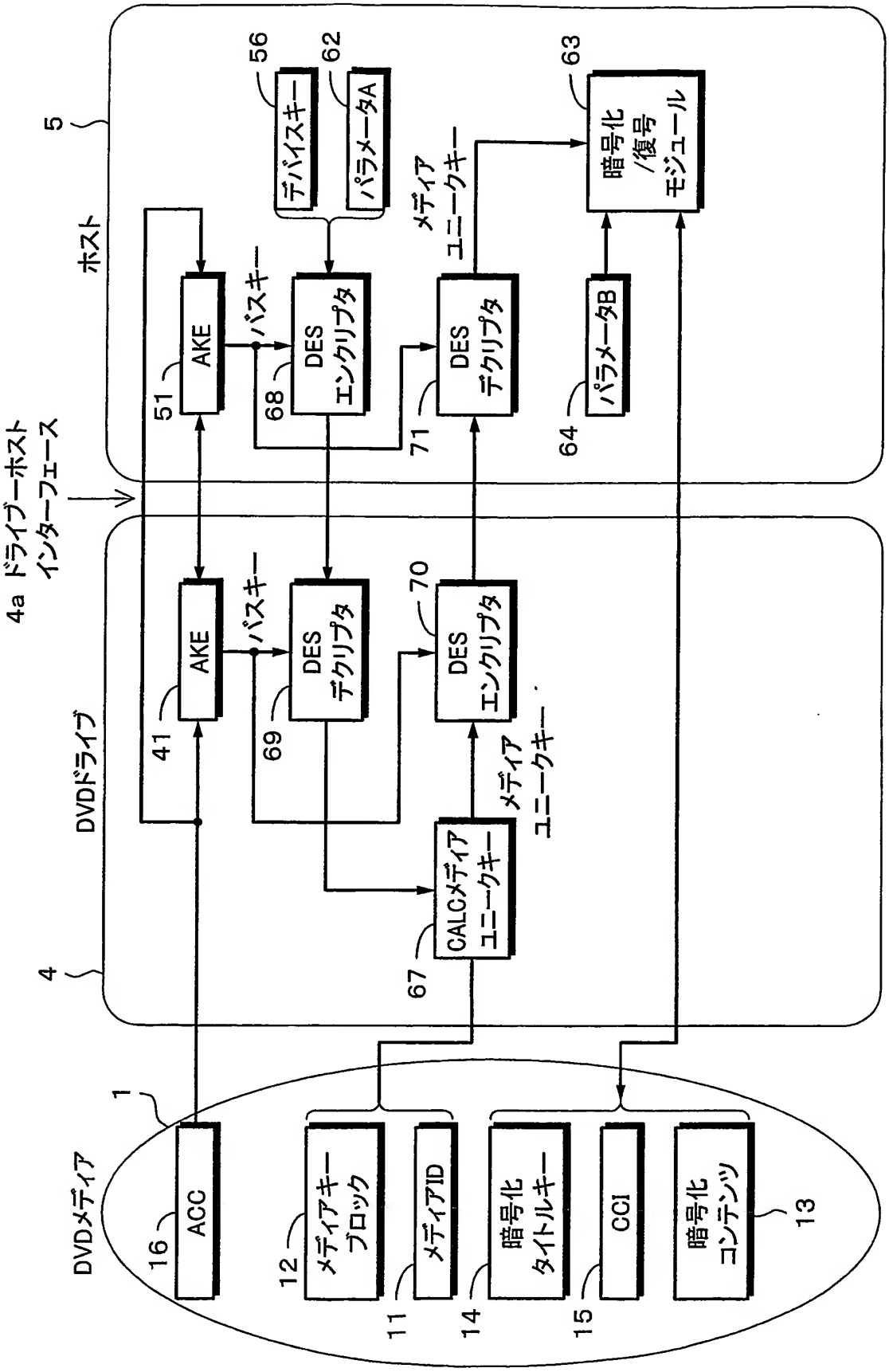
第１３図


DVDメディア
1
ACC
16
メディアキーブロック
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
4
DVDドライブ
AKE
41
バスキー
MAC
42
DES エンクリプタ
65
デバイスキー
46
パラメータA
62
パラメータB
64
4a ドライブーホストインターフェース
5
ホスト
AKE
51
バスキー
MAC
52
比較
53
SW3
DES デクリプタ
66
SW1
パラメータB
デバイスキー パラメータA
CALCメディアユニークキー
61
メディアユニークキー
暗号化/復号モジュール
63

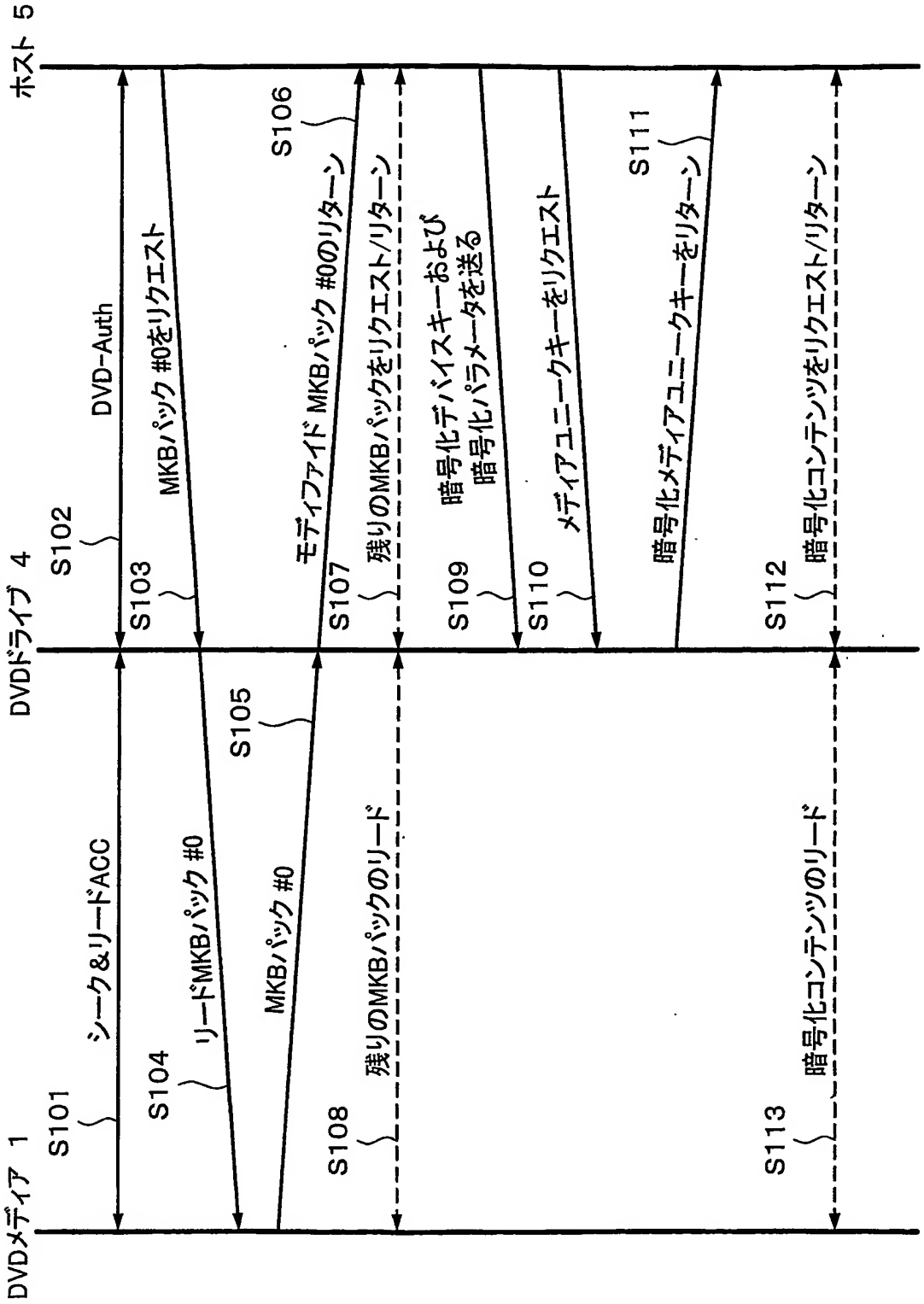
第１４図


ホスト 5
DVDドライブ 4
DVDメディア 1
S81
シーク&リードACC
S82
DVD-Auth
S83
MKBパック #0をリクエスト
S84
リードMKBパック #0
S85
MKBパック #0
S86
モディファイド MKBパック #0のリターン
S87
S88
残りのMKBパックのリード
S89
残りのMKBパックをリクエスト/リターン
S90
メディアIDをリード
S91
メディアID
S92
メディアIDとmlをリターン
S93
デバイスキーおよびパラメータをリクエスト
S94
暗号化データをリターン
S95
暗号化コンテンツをリクエスト/リターン
S96
暗号化コンテンツのリード
メディアIDをリクエスト

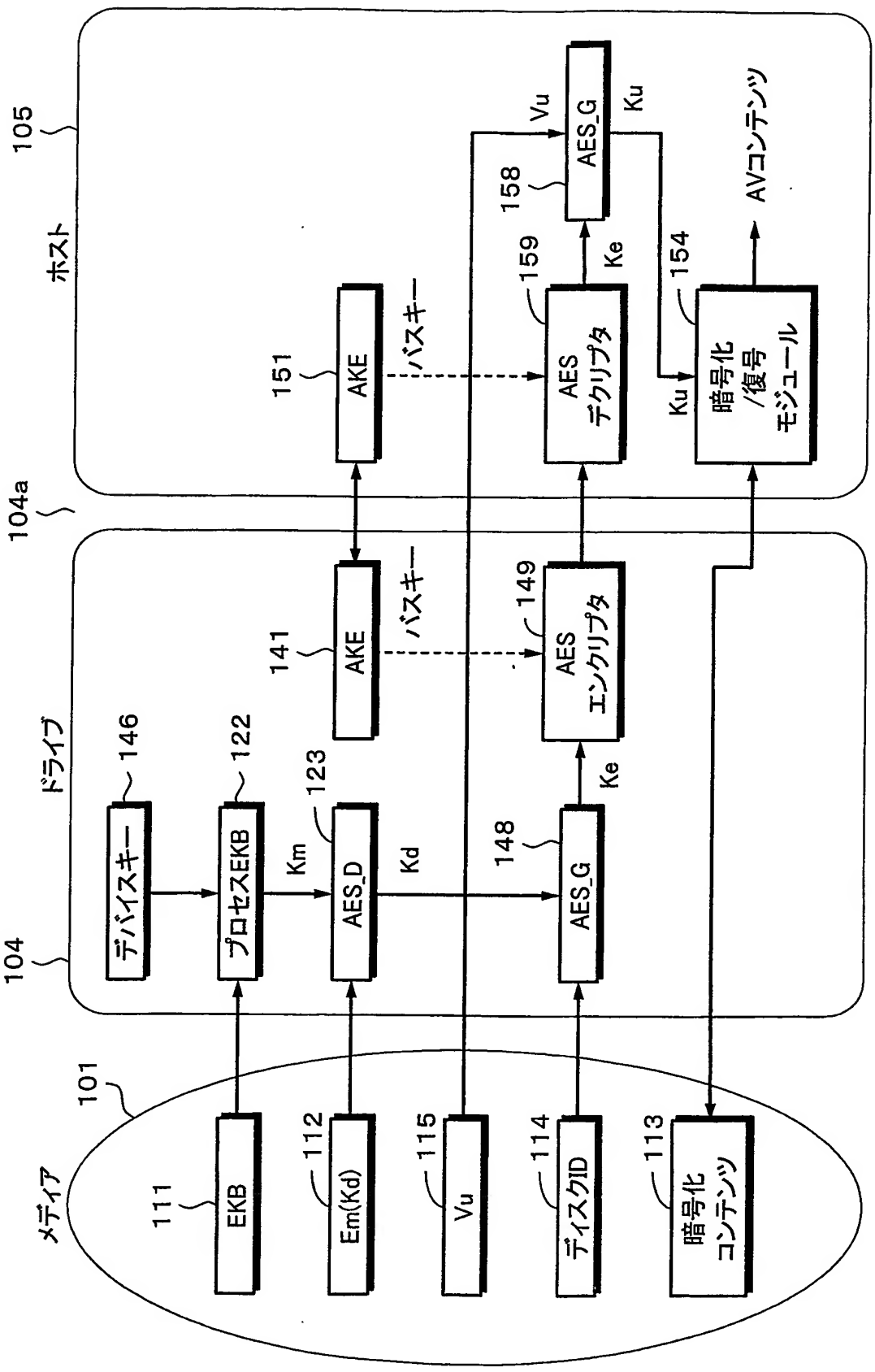
第１５図


5
ホスト
56
デバイスキー
62
パラメータA
63
暗号化
/復号
モジュール
メディア
ユニークキー
AKE
51
バスキー
DES
エンクリプタ
68
DES
デクリプタ
71
パラメータB
64
4a ドライブーホスト
インターフェース
DVDドライブ
AKE
41
バスキー
DES
デクリプタ
69
DES
エンクリプタ
70
メディア
ユニークキー
CALCメディア
ユニークキー
67
4
1
DVDメディア
ACC
16
メディアキー
ブロック
12
メディアID
11
暗号化
タイトルキー
14
CCI
15
暗号化
コンテンツ
13

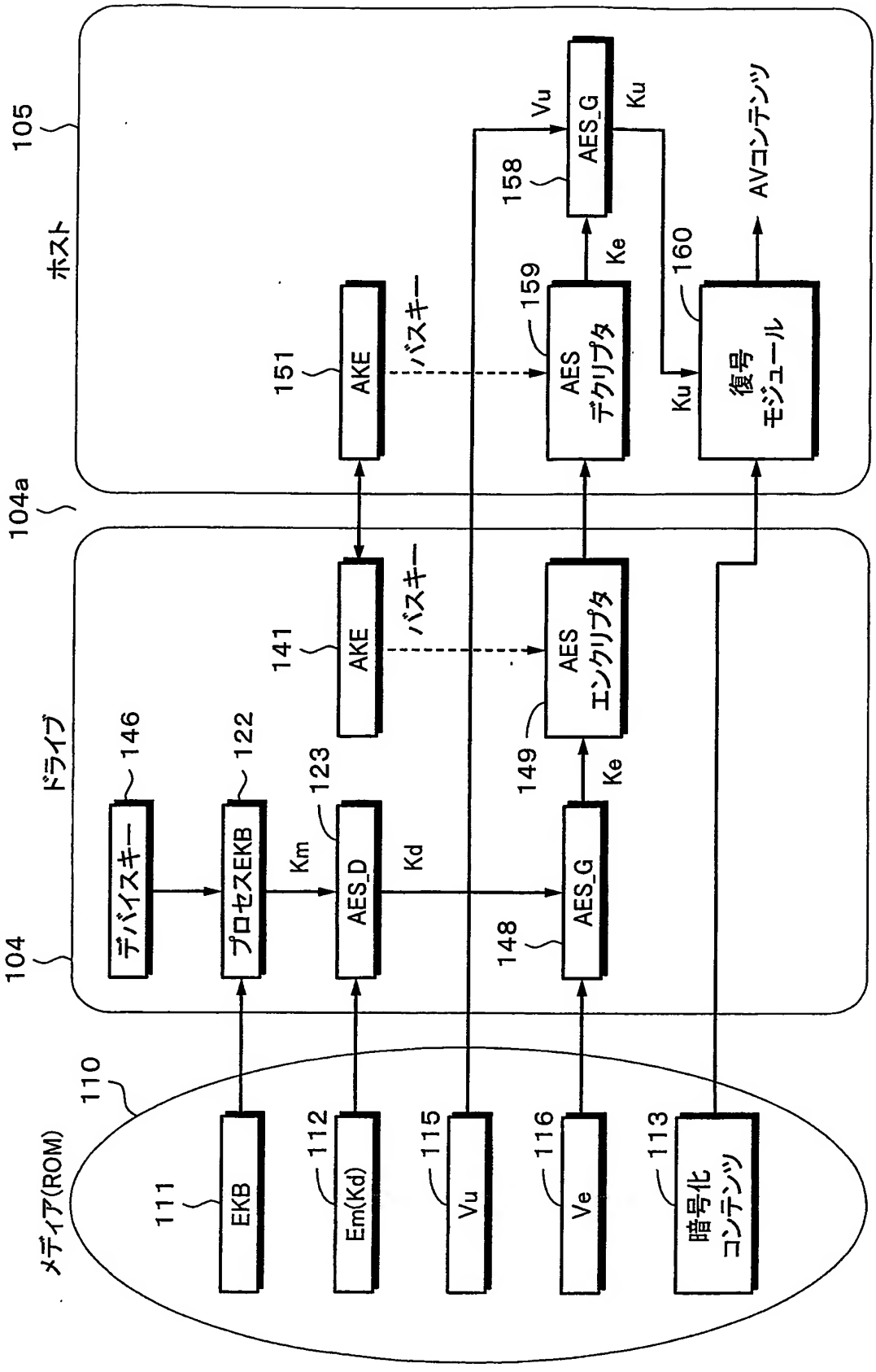
第１６図


ホスト 5
DVDドライブ 4
DVDメディア 1
S101
シーク&リードACC
S102
DVD-Auth
S103
MKBパック #0をリクエスト
S104
リードMKBパック #0
S105
MKBパック #0
S106
モディファイド MKBパック #0のリターン
S107
残りのMKBパックをリクエスト/リターン
S108
残りのMKBパックのリード
S109
暗号化デバイスキーおよび
暗号化パラメータを送る
S110
メディアユニークキーをリクエスト
S111
暗号化メディアユニークキーをリターン
S112
暗号化コンテンツをリクエスト/リターン
S113
暗号化コンテンツのリード

第１７図


メディア
101
111
EKB
112
Em(Kd)
115
Vu
114
ディスクID
113
暗号化
コンテンツ
ドライブ
104
デバイスキー
146
プロセスEKB
122
Km
123
AES_D
Kd
141
AKE
バスキー
148
AES_G
Ke
149
AES
エンクリプタ
104a
ホスト
105
151
AKE
バスキー
159
AES
デクリプタ
Ke
158
AES_G
Vu
Ku
154
Ku
暗号化
/復号
モジュール
AVコンテンツ

第１８図


メディア(ROM)
110
EKB
111
Em(Kd)
112
暗号化
コンテンツ
113
Vu
115
Ve
116
ドライブ
104
デバイスキー
146
プロセスEKB
122
AES_D
123
Km
Kd
AES_G
148
AES
エンクリプタ
149
Ke
AKE
141
バスキー
ホスト
104a
AKE
151
バスキー
AES
デクリプタ
159
Ke
AES_G
158
Vu
Ku
復号
モジュール
160
Ku
AVコンテンツ
105

符号の説明

ＳＴ１　ＭＡＣ計算値が一致？

ＳＴ２　スイッチをＯＮ

ＳＴ３　スイッチをＯＦＦ

１　ＤＶＤメディア　２　レコーダ　３　プレーヤ

４　ＤＶＤドライブ　４ａ　インターフェース　５　ホスト

１１　メディアＩＤ　１２　メディアキーブロック（ＭＫＢ）

１３　暗号化コンテンツ　４２，５２　ＭＡＣ演算ブロック

４６　デバイスキー　４６ａ　デバイスキーの前半部

４７　ＤＥＳエンクリプタ

４８　メディアユニークキー演算ブロック

４９，４９ａ　ＤＥＳエンクリプタ

４９ｂ　ＤＥＳデクリプタ　５３　ＭＡＣを比較する比較

５４　暗号化／復号モジュール

５５　メディアユニークキー演算ブロック

５６ａ　デバイスキーの後半部　５７　ＤＥＳデクリプタ

５８　デバイスキー合成部　５９，５９ａ　ＤＥＳデクリプタ

６１　メディアユニークキー演算ブロック

６２　パラメータＡ　６３　暗号化／復号モジュール

６４　パラメータＢ　６５　ＤＥＳエンクリプタ

６６　ＤＥＳデクリプタ

１０１　メディア　１０４　ドライブ　１０５　ホスト

１１１　ＥＫＢ　１１２　暗号化ディスクキー

１１３　暗号化コンテンツ　１１４　ディスクＩＤ

１１５　ユニットキー生成用値　１１６　エンベディッドキー生成値